Diffusion en mode commutation de circuits dans les tores de dimension k

Olivier Delmas et Stéphane Perennes

Projet SLOOP *
Laboratoire I3S - CNRS URA 1376
930 Route des Colles, B.P. 145
06903 Sophia Antipolis Cedex
Courrier électronique : {delmas, sp}@unice.fr.

* SLOOP (Simulation, Langages Orientés Objets et Parallélisme) est un projet commun entre le CNRS, l'INRIA et l'Université de Nice - Sophia Antipolis.

RÉSUMÉ. *Dans cet article, nous étudions la diffusion en mode commutation de circuits dans le tore de dimension k en supposant qu'un nœud peut envoyer des messages simultanément sur tous ses canaux de sortie. Nous considérons le protocole de diffusion comme une succession d'étapes et durant chacune d'elles les communications se font selon des chemins arc-disjoints. Nous donnons des protocoles de diffusion optimaux en nombre d'étapes et quasi-optimaux pour les longueurs des chemins. Ceci généralise le résultat de Peters et Syska [PET 96] obtenu pour $k = 2$. Pour ce faire, nous utilisons des codes linéaires. Nous détaillons en particulier les cas des tores de dimension 3 et 4.*

ABSTRACT. *This paper deals with broadcasting in k−dimensional torus network under the circuit-switched routing model. We suppose that a node can send a message simultaneously on all its out-links. Here, we consider a broadcast protocol as a succession of rounds ; during each round, the communication dipaths used by the algorithm must be arc-disjoint. We give optimal protocols for the number of rounds and near of the optimal for the length of communication dipaths. This work generalizes that of Peters and Syska [PET 96] concerning the case $k = 2$. We use tools of linear coding theory and describe in details the cases $k = 3$ and $k = 4$.*

MOTS-CLÉS : *diffusion, commutation de circuits, tore, théorie des codes.*

KEY WORDS : *broadcasting, circuit-switching, torus network, coding theory.*

1. Introduction

En algorithmique parallèle et distribuée il est important de disposer d'une part d'un protocole de routage efficace (fonction de routage) [FRA 95] et d'autre part d'algorithmes de communications globales [PER 96]. L'étude d'algorithmes classiques montre qu'il existe un certain nombre de communications globales qui apparaissent très souvent, par exemple en algèbre linéaire ou non-linéaire, ou en traitement d'images. Un problème classique de communications généralisées ou globales couramment rencontré [MCK 94, RUM 94] est **la diffusion** (un processeur envoie son message à destination de tous les autres processeurs). Mais les algorithmes dépendent fortement du mécanisme de routage des messages utilisés. Dans cet article nous nous intéressons à la diffusion sur les réseaux toriques qui utilisent un routage de type commutation de circuits. En effet, ce routage, déjà bien connu dans les réseaux de télécommunications est désormais utilisé sur des machines parallèles les plus récentes telles que l'IBM SP2, la Paragon d'Intel ou les deux dernières générations de Cray (T3D et T3E). De plus les réseaux toriques, par leur simplicité et leur importance dans de nombreuses applications numériques, constituent une architecture souvent utilisée (par exemple, les Cray T3D et T3E utilisent une topologie en tore de dimension 3).

1.1. *Modélisation du problème*

1.1.1. *Le modèle de type commutation de circuits*

Nous regrouperons sous le terme **« routage de type commutation de circuits »**, les routages par *commutation de circuits*, *wormhole* [SEI 90], *virtual cut-through* [KER 79] ou *direct connect* [NUG 88]. Bien qu'il existe des différences entre ces diverses techniques (par exemple: présence ou non d'un accusé de réception, faible ou grande taille des tampons d'entrée et de sortie des liens, etc), pour l'étude des communications globales, les différences entre ces modes de routage apparaissent comme trop fines et en tout état de cause difficilement modélisables pour être prises en compte dans une étude théorique.

Dans le but de pouvoir comparer les divers protocoles proposés et d'évaluer leur qualité, il est nécessaire d'adopter un modèle commun. Ceci a déterminé la plupart des auteurs à se placer dans le cadre du « modèle de type commutation de circuits » qui est désormais le plus communément adopté. Celui-ci consiste à dire que les **protocoles de communications globales s'effectuent comme une succession d'étapes.** Une étape comporte généralement plusieurs communications entre divers couples de sommets. Ces communications, pour éviter des blocages ou des pertes, devront s'effectuer le long de **chemins arc-disjoints.** Notons que certains auteurs imposent une contrainte plus forte, en considérant des chemins sommet-disjoints [FEL 93]. Le coût d'une étape est le maximum du coût des communications ayant lieu au cours de cette étape. Souvent, il est pratique de considérer qu'**une étape ne peut commencer que si toutes les communications de l'étape précédente sont achevées**. Dans ce cas, on dit que les protocoles sont « synchrones ».

Dans la suite, nous regrouperons les routages du « type commutation de circuits synchrone » sous le terme `mode commutation de circuits`.

1.1.2. *Temps de communication d'un processeur à un autre*

Dans le mode commutation de circuits, lorsqu'un processeur envoie un message à un autre processeur, la modélisation du temps de transmission s'exprime comme la somme de trois termes : le premier tient compte d'un délai constant, aussi appelé délai d'initialisation, induit par le processus qui envoie le message, le second est associé au temps de commutation des commutateurs par lesquels transite le message et le troisième mesure le débit de l'information. Ainsi, pour un message de longueur L allant d'un processeur x à un processeur y, le long d'un chemin de longueur l, le temps de communication sera modélisé par $T_{x\to y} = \alpha + l\delta + L\tau$ (modèle linéaire complet), où α est le délai d'initialisation, δ le temps de commutation d'un commutateur intermédiaire et $\frac{1}{\tau}$ la bande passante des liens.

Il existe diverses simplifications de ce modèle de temps (justifiées par la réalité). Celle que nous adopterons dans cette étude consiste à considérer un message de petite longueur pour lequel $\alpha >> L\tau$ et $l\delta >> L\tau$. Le modèle de temps peut alors se réduire à $T_{x\to y} = \alpha + l\delta$. Le cas des messages longs se traite généralement avec des techniques très différentes du type *"pipe-line"* (arbres couvrants arc-disjoints, ...) [RUM 94] ; nous ne les aborderons pas ici.

1.1.3. *Contraintes du réseau*

Les résultats dépendent aussi de la modélisation de la topologie du réseau et des contraintes technologiques qui lui sont associées. Le réseau sera modélisé ici par un graphe orienté $G = (V, A)$ qui sera supposé symétrique et dont l'ensemble V des sommets représentent les commutateurs et l'ensemble A des arcs les liaisons entre les "tampons d'entrée et sortie" de ces commutateurs.

Suivant la conception du réseau modélisé, il peut exister des restrictions sur les capacités d'émission et de réception de chaque processeur. Le cas où l'on autorise au maximum une émission et une réception a été étudié dans la littérature [BAR 96]. Comme cette étude s'inscrit en continuité des travaux de [PET 96], nous utiliserons les mêmes hypothèses de modélisation des contraintes des réseaux qu'eux. Ainsi, nous supposerons que l'on peut émettre sur tous les canaux de sortie (mode appelé $\Delta-$ports). Notons que dans un protocole de diffusion lorsque l'on ne s'autorise pas le découpage du message, il n'y a pas de contrainte sur la réception, car il suffit que le message arrive une et une seule fois sur un processeur.

1.1.4. *Protocole de diffusion*

Soit G un graphe orienté symétrique et sommet transitif. Alors dans le mode commutation de circuits, nous pouvons définir le coût d'un protocole de diffusion ainsi.

Notation 1 Le temps (ou coût) d'un algorithme de diffusion dans un graphe G, noté $b(G)$, est le temps nécessaire induit par l'algorithme pour effectuer la diffusion

dans G à partir d'un sommet quelconque. Dans le modèle linéaire complet, ce temps s'exprime comme la somme de trois termes : $b(G) = b_\alpha(G)\alpha + b_\delta(G)\delta + b_\tau(G)L\tau$, où $b_\alpha(G)$ représente le nombre d'étapes de l'algorithme, $b_\delta(G)$ la somme du maximum des distances des communications entre processeurs impliqués à chaque étape de l'algorithme et $b_\tau(G)$ mesure le flot d'information.

Conformément à notre modèle de temps, nous ne prendrons en compte que les cœfficients $b_\alpha(G)$ et $b_\delta(G)$. Dans [DEL 97] il est montré, sous certaines conditions, que l'optimum en nombre d'étapes ne peut être atteint que si l'on ne découpe pas le message, auquel cas $b_\alpha(G) = b_\tau(G)$.

1.2. *Définitions et notations*

Nous utiliserons les définitions et notations suivantes :

• $\mathbb{Z}_q$ représente le groupe additif des **entiers modulo q**. Les représentants de $\mathbb{Z}_q$ seront notés $\{0, 1, \ldots, q-1\}$ dans le cas général. Mais dans le cas qui se révèlera ici le plus étudié, c'est-à-dire lorsque $q = 2k+1$, nous prendrons comme représentants canoniques les nombres $\{-k, \ldots, 0, \ldots, k\}$ (ceci pour des raisons de représentation géométrique, de manière à avoir le 0 au centre des figures, voir figure 1).
• G représente un graphe orienté symétrique. $V(G)$ et $A(G)$ représentent respectivement l'**ensemble des sommets** et l'**ensemble des arcs** de G.
• N représente le **nombre de sommets de** G : $N = |V(G)|$.
• $d_G(x, y)$ représente la **distance** d'un sommet $x \in V(G)$ à un sommet $y \in V(G)$ définie comme étant la longueur du plus court chemin allant de x à y.
• $D(G)$ représente le **diamètre** du graphe G, c'est-à-dire le maximum des distances pris entre chaque couple de sommets : $D(G) = max_{(x,y)\in V^2(G)} d_G(x, y)$.
• Dans un graphe orienté symétrique G, $\Delta(G)$ (aussi noté Δ) représente le **degré entrant (ou sortant) maximum** dans G, c'est-à-dire le maximum des degrés entrants (ou sortants) de tous les sommets de G.
• C_N représente le **circuit symétrique** d'ordre N (voir figure 1-a et 1-b).

Définition 1 [RUM 94] *La* **somme cartésienne** *de deux graphes orientés G et G', que nous noterons $G \square G'$, est le graphe orienté dont tous les sommets sont tous les couples (x, x') où x est un sommet de G et x' est un sommet de G'. Le sommet (y, y') est un successeur du sommet (x, x') dans $G \square G'$ si et seulement si $x = y$ et (x', y') est un arc de G' ou si $x' = y'$ et (x, y) est un arc de G.*

Définition 2 *Un* **tore de dimension** k *est la somme cartésienne de k circuits symétriques d'ordre $l_1, l_2, \ldots, l_k$ et sera noté par $TM(l_1, l_2, \ldots, l_k) = C_{l_1} \square C_{l_2} \square \cdots \square C_{l_k}$.*

Remarque 1 Si pour $1 \leq i \leq k$, $l_i \geq 3$, le tore est alors un graphe orienté régulier de degré $\Delta = 2k$. Son ordre est $l_1 \times l_2 \times \cdots \times l_k$, le nombre d'arcs est $2kN$ et son diamètre est $\sum_{i=1}^{i=k} \lfloor \frac{l_i}{2} \rfloor$.

Notation 2 *Lorsque $l_1 = l_2 = \cdots = l_k = l$, nous utiliserons la notation condensée $TM(l)^k$ et supposerons dans ce qui suit que $l \geq 3$ (voir figure 1). Nous appelerons ces graphes des* **tores carrés de coté l et de dimension k.**

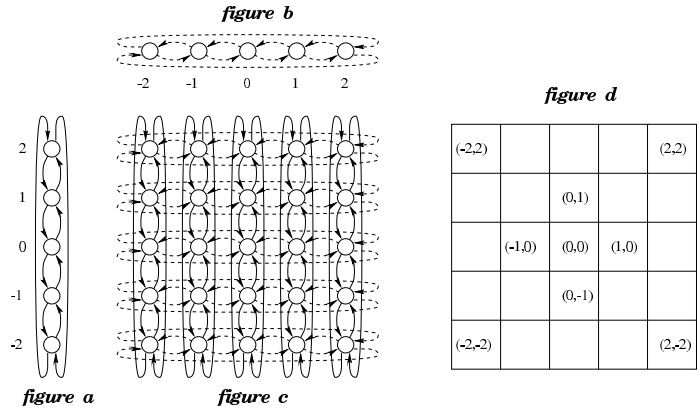

Fig 1 - *Les* `figures-a` *et* `b` *représentent deux circuits symétriques d'ordre 5 notés* C_5. *La* `figure-c` *représente le tore carré de dimension 2 et de coté 5. Ce tore est la somme cartésienne des 2 circuits symétriques* C_5, *soit* $TM(5)^2 = TM(5,5) = C_5 \square C_5$. *Par souci de clarté, nous pourrons choisir de représenter les tores en omettant de dessiner les arcs et en assimilant les sommets à des carrés. Un exemple d'une telle représentation est donné pour le tore* $TM(5)^2$ *en* `figure-d`, *avec les éléments de* $\mathbb{Z}_5$ *noté* $\{-2,-1,0,1,2\}$.

Remarque 2 Chaque sommet x du tore $TM(l_1, l_2, \cdots, l_k)$ peut être vu comme un vecteur de dimension k noté $(x_1, x_2, \cdots, x_k) \in \mathbb{Z}_{l_1} \times \mathbb{Z}_{l_2} \times \cdots \times \mathbb{Z}_{l_k}$. Chaque sommet $(x_1, x_2, \cdots, x_k)$ est joint par un arc aux $2k$ sommets $(x_1, x_2, \cdots, x_i \pm 1, \cdots, x_k)$ pour $1 \leq i \leq k$.

Remarque 3 Comme le tore $TM(l)^k$ est un graphe sommet-transitif, nous considérerons dans la suite, que dans tout protocole de diffusion le sommet émetteur est le vecteur nul que nous noterons 0.

1.3. *Etat de l'art pour le modèle Δ-ports en commutation de circuits*

Pour un nombre fixé d'étapes T dans un protocole de diffusion, le nombre maximum potentiel de sommets susceptible de recevoir le message est majoré par $(\Delta+1)^T$. On a donc $b_\alpha(G) \geq \lceil \log_{\Delta+1} N \rceil$. Une borne inférieure sur la longueur des chemins est $b_\delta(G) \geq D(G)$.

La détermination de la valeur $b_\alpha(G)$ optimale est un problème parfois ardu. La minimisation simultanée des deux paramètres $b_\alpha(G)$ et $b_\delta(G)$ est encore plus difficile et ce problème a été peu étudié. Jusqu'à présent, seuls certains cas particuliers ont été examinés. Pour le circuit symétrique C_N, on obtient facilement que $b_\alpha(C_N) = \lceil \log_3 N \rceil$ avec une longueur totale de chemin optimale. La diffusion dans l'hypercube a été étudiée dans [HO 95]. Leurs auteurs donnent un algorithme asymptotiquement optimal en nombre d'étapes. Il semble difficile d'obtenir sur tout hypercube de dimension quelconque un algorithme de diffusion optimal pour le nombre d'étapes. Néanmoins, Kodate [KOD 96] a obtenu des algorithmes optimaux en nombre d'étapes sur

des hypercubes dont les dimensions sont de la forme 2^k+1, en utilisant des codes cycliques. Le lecteur pourra trouver une synthèse plus complète de ces problèmes dans [DEL 97, FLE 96] et dans le papier [CAS] en préparation. Dans le cas des tores de dimension k, le nombre maximum de sommets que l'on peut atteindre en T étapes est $(2k+1)^T$. Nous nous limiterons donc dans la suite à l'étude du cas critique de la diffusion dans les tores carrés de coté $(2k+1)^i$ et de dimension k. En ce qui concerne les tores de dimension 2, Peters et Syska ont exhibé [PET 96] un algorithme optimal à la fois pour le nombre d'étapes et la longueur des chemins pour les tores carrés de coté $l=5^i$, i.e. $b_\alpha(TM(l)^2)=2\log_5(l)=2i$ et $b_\delta(TM(l)^2)=D(TM(l)^2)=l-1$. Dans le cas général, Park et Choi [PAR 94, PAR 96] proposent un algorithme optimal en nombre d'étapes sur le tore $TM((2k+1)^i)^k$, mais sans tenir compte de la longueur des chemins. Pour notre part, nous avons étudié de façon indépendante le même problème et nous montrons que l'on peut exhiber des algorithmes optimaux en nombre d'étapes, à savoir $b_\alpha(G)=ki$, pour $G=TM((2k+1)^i)^k$, mais pour un $b_\alpha(G)$ optimal nous essayons de minimiser le paramètre $b_\delta(G)$.

2. Principe général de la diffusion dans les tores carrés de dimension k

Nous donnons ici une manière de construire un protocole dans le tore carré de coté $l_1 \times l_2$ et de dimension k, connaissant un protocole dans le tore carré de coté l_1 et de dimension k et dans le tore carré de coté l_2 et de dimension k.

Lemme 1 – Notons par $G_l^k = TM(l)^k$ le tore carré de coté l et de dimension k. Alors il existe un algorithme de diffusion dans $G^k_{l_1\times l_2}$ vérifiant :

i)	nombre d'étapes	$b_\alpha(G^k_{l_1\times l_2})$	$\leq$	$b_\alpha(G^k_{l_1})$	$+$	$b_\alpha(G^k_{l_2})$,
ii)	longueur des chemins	$b_\delta(G^k_{l_1\times l_2})$	$\leq$	$l_2 \cdot b_\delta(G^k_{l_1})$	$+$	$b_\delta(G^k_{l_2})$.

Preuve. De manière intuitive, on va décomposer le tore $G^k_{l_1\times l_2}$ en l_1^k sous-grilles ayant l_2^k sommets. Le sommet initiateur informera dans une première phase un élément de chaque sous-grille en suivant un protocole analogue à celui de $G^k_{l_1}$. Puis dans une seconde phase, les sommets connaissant l'information informeront en parallèle leur "voisinage local" suivant un protocole analogue à celui de $G^k_{l_2}$.

Plus formellement, considérons la bijection de $\mathbb{Z}_{l_1\times l_2}$ dans $\mathbb{Z}_{l_1}\times\mathbb{Z}_{l_2}$ qui à l'élément $z\in\{0,\ldots,l_1\times l_2-1\}$ associe le couple (x,y) avec $x\in\{0,\ldots,l_1-1\}$ et $y\in\{0,\ldots,l_2-1\}$ défini par $z=x\cdot l_2+y$. Par exemple avec $l_1=2$ et $l_2=3$, la bijection de $\mathbb{Z}_6$ dans $\mathbb{Z}_2\times\mathbb{Z}_3$ associe à $0\to(0,0)$; $1\to(0,1)$; $2\to(0,2)$; $3\to(1,0)$; $4\to(1,1)$; $5\to(1,2)$. Avec cette bijection, un arc de z à $z+1$ dans $C_{l_1\times l_2}$ devient l'arc de (x,y) à $(x,y+1)$ si $0\leq y<l_2-1$ ou bien de (x,l_2-1) à $(x+1,0)$ si $y=l_2-1$. De même, un arc de z à $z-1$ dans $C_{l_1\times l_2}$ devient l'arc de (x,y) à $(x,y-1)$ si $0<y\leq l_2-1$ ou bien de $(x,0)$ à $(x-1,l_2-1)$ si $y=0$. Avec l'exemple précédent dans C_6, l'arc allant de 5 à 0 dans $\mathbb{Z}_6$ devient l'arc allant de $(1,2)$ à $(0,0)$ dans $\mathbb{Z}_2\times\mathbb{Z}_3$. Plus généralement à l'élément $(z_1,z_2,\ldots,z_k)$ de $\mathbb{Z}^k_{l_1\times l_2}$, nous associerons l'élément $(x_1,y_1),\ldots,(x_i,y_i),\ldots,(x_k,y_k)$ avec $(x_1,\ldots,x_i,\ldots,x_k)\in\mathbb{Z}^k_{l_1}$ et

$(y_1,\ldots,y_i,\ldots,y_k) \in \mathbb{Z}_{l_2}^k$. Le graphe induit par les sommets de la forme $(x_1,0),\ldots,(x_k,0)$ pour tout $(x_1,\ldots,x_k) \in \mathbb{Z}_{l_1}^k$ forme un tore dilaté, c'est-à-dire qu'il est obtenu à partir de $G_{l_1}^k$ en remplaçant chaque arc par un chemin de longueur l_2. Plus exactement, l'arc allant de $(x_1,\ldots,x_i,\ldots,x_k)$ à $(x_1,\ldots,x_i+1,\ldots,x_k)$ dans $G_{l_1}^k$ correspond à un chemin de longueur l_2 dans $G_{l_1\times l_2}^k$ reliant $(x_1,0),\ldots,(x_i,0),\ldots,(x_k,0)$ à $(x_1,0),\ldots,(x_i+1,0),\ldots,(x_k,0)$ via les sommets intermédiaires $(x_1,0),\ldots,(x_{i-1},0),(x_i,y_i),(x_{i+1},0),\ldots(x_k,0)$ en utilisant tout les y_i allant de 1 à l_2-1.

Dans une première phase on va appliquer un protocole identique au protocole de diffusion dans $G_{l_1}^k$ de manière à ce que le sommet $(0,0),\ldots,(0,0),\ldots,(0,0)$ informe tous les sommets $(x_1,0),\ldots,(x_i,0),\ldots,(x_k,0)$ pour tout $(x_1,\ldots,x_k) \in \mathbb{Z}_{l_1}^k$. Pour cela, si dans $G_{l_1}^k$ à l'étape t le sommet $(x_1,\ldots,x_k)$ informe le sommet $(x'_1,\ldots,x'_k)$ via un chemin de longueur d ; alors dans $G_{l_1\times l_2}^k$ à l'étape t le sommet $(x_1,0),\ldots,(x_k,0)$ informera le sommet $(x'_1,0),\ldots,(x'_k,0)$ via un chemin de longueur $d\cdot l_2$. Cette phase s'effectue donc en $b_\alpha(G_{l_1}^k)$ étapes avec un cœfficient en longueur de chemins égal à $l_2 \cdot b_\delta(G_{l_1}^k)$. Dans l'exemple avec $l_1 = 2$ et $l_2 = 3$ supposons que dans G_2^2 le sommet $(0,0)$ informe $(1,0)$ et $(1,1)$ par le chemin de longueur 2 utilisant le sommet intermédiaire $(0,1)$ (Cf. figure 2-a), alors dans G_6^2 le sommet $(0,0),(0,0)$ informera $(1,0),(0,0)$ via un chemin de longeur 3 et $(1,0),(1,0)$ via un chemin de longueur 6 (Cf. figure 2-b).

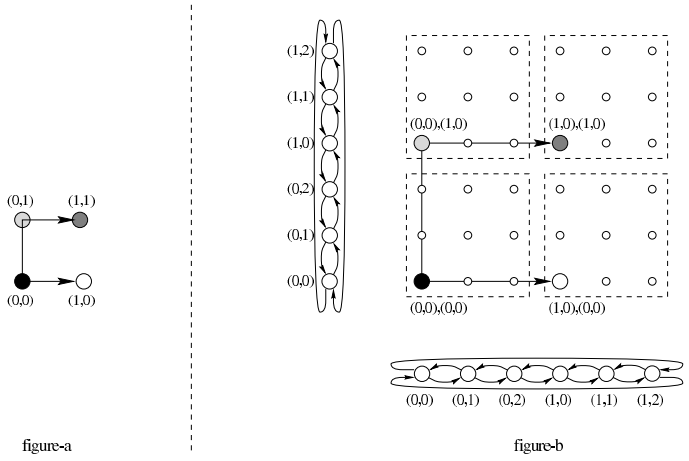

Fig 2 - *Exemple de première phase. La* `figure-a` *représente les chemins de communications issus du sommet* $(0,0)$ *dans* G_2^2. *La* `figure-b` *montre que les chemins de communications dans* G_6^2 *issus du sommet* $(0,0),(0,0)$ *correspondent aux schémas induits par ceux dans* G_2^2, *mais avec un facteur de dilatation de 3.*

Dans une seconde phase, les sommets informés $(x_1,0),\ldots,(x_k,0)$ vont diffuser en parallèle le message à leurs "voisins" en utilisant le protocole dans $G_{l_2}^k$. Intuitivement on voudrait que le sommet $(x_1,0),\ldots,(x_k,0)$ informe les l_2^k sommets $(x_1,y_1),\ldots,$

(x_k, y_k) pour tout $(y_1, \ldots, y_k) \in \mathbb{Z}_{l_2}^k$ de la même manière que le sommet $(0, \ldots, 0)$ informait les sommets $(y_1, \ldots, y_k)$ dans $G_{l_2}^k$. Ceci n'est pas possible tel quel car le graphe engendré par les sommets $(x_1, y_1), \ldots, (x_k, y_k)$ est une sous-grille non torique, et on ne peut pas appliquer strictement le protocole de $G_{l_2}^k$ si un chemin de la diffusion utilise un arc de "rebouclement" de la forme $(y_1, \ldots, y_i, \ldots, y_k), (y_1, \ldots, y_i + 1, \ldots, y_k)$ avec $y_i = l_2 - 1$ et $y_i + 1 = 0$ (ou un arc opposé). Néanmoins, on peut utiliser un arc aboutissant dans une sous-grille voisine et chaque sommet informera alors l_2^k sommets même si ceux-ci n'appartiennent pas tous à la même sous-grille. Formellement, supposons que dans $G_{l_2}^k$ à l'étape t, le sommet $(y_1, \ldots, y_k)$ informe le sommet $(y'_1, \ldots, y'_k)$ alors dans $G_{l_1 \times l_2}^k$ le sommet $(x_1, y_1), \ldots, (x_i, y_i), \ldots, (x_k, y_k)$ informera le sommet $(x_1^*, y'_1), \ldots, (x_i^*, y'_i), \ldots, (x_k^*, y'_k)$ avec $x_i^* = x_i$ si dans $G_{l_2}^k$ le chemin utilise seulement des arcs de la forme $(y_1, \ldots, y_i, \ldots, y_k)$ à $(y_1, \ldots, y_i \pm 1, \ldots, y_k)$ avec $0 < y_i < l_2 - 1$, ou bien $x_i^* = x_i + 1$ si le chemin utilise un arc de la forme $(y_1, \ldots, y_i, \ldots, y_k)$ à $(y_1, \ldots, y_i + 1, \ldots, y_k)$ avec $y_i = l_2 - 1$ et $y_i + 1 = 0$, ou enfin $x_i^* = x_i - 1$ si le chemin utilise un arc de la forme $(y_1, \ldots, y_i, \ldots, y_k)$ à $(y_1, \ldots, y_i - 1, \ldots, y_k)$ avec $y_i = 0$ et $y_i - 1 = l_2 - 1$. Dans notre exemple, supposons que dans G_3^2 le sommet $(0,0)$ informe $(0,1)$; $(1,1)$ via le sommet $(1,0)$; $(1,2)$ via le sommet $(0,2)$ et $(2,1)$ via les sommets $(2,0)$ et $(2,2)$ (Cf. figure 3-a), alors dans G_6^2, le sommet $(0,0), (0,0)$ informera le sommet $(0,0), (0,1)$; $(0,1), (0,1)$ via le sommet $(0,1), (0,0)$, mais il informera le sommet $(0,1), (1,2)$ (ici $x_2^* = x_2 - 1$) via le sommet $(0,0), (1,2)$ et il informera le sommet $(1,2), (1,1)$ (ici $x_1^* = x_1 - 1$ et $x_2^* = x_2 - 1$) via les sommets $(1,2), (0,0)$ et $(1,2), (1,2)$ (Cf. figure 3-b).

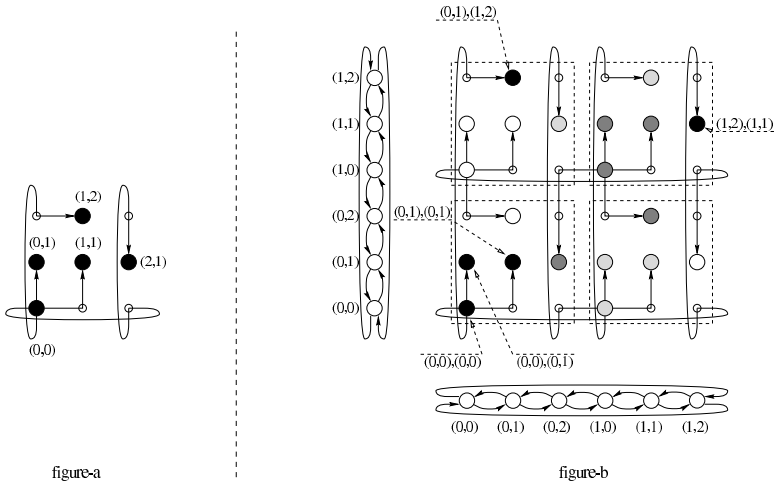

Fig 3 - *Exemple d'une étape de la seconde phase. La* `figure-a` *représente les chemins de communications issus du sommet* $(0,0)$ *dans* G_3^2 *(en une étape). La* `figure-b` *montre que les chemins de communications dans* G_6^2 *(en une étape) qui sont issus des sommets* $(x_1, 0), (x_2, 0)$ *avec* $(x_1, x_2) \in \mathbb{Z}_2^2$ *correspondent aux schémas induits par ceux dans* G_3^2*. Au cours de cette étape, ces chemins sont tous arc-disjoints.*

De la même manière le sommet $(x_1,0),(x_2,0)$ informera les 4 sommets $(x_1,0),(x_2,1)$; $(x_1,1),(x_2,1)$; $(x_1,1),(x_2-1,2)$ et $(x_1-1,2),(x_2-1,1)$ (Cf. figure 3-b). A une étape t les chemins issus du sommet $(0,0),\ldots,(0,0)$ sont deux à deux disjoints, car les chemins dans $G^k_{l_2}$ étaient deux à deux disjoints. Les chemins issus d'un autre sommet $(x_1,0),\ldots,(x_k,0)$ sont obtenus par translation des chemins issus de $(0,0),\ldots,(0,0)$ et tous ces chemins sont bien deux à deux arc-disjoints. □

Cette première propriété nous permet de concevoir une méthode de diffusion récursive sur les tores carrés de coté l^i et de dimension k.

Proposition 1 – Soit $G^k_{l^i} = TM(l^i)^k$. Il existe un protocole de diffusion dans $G^k_{l^i}$ tel que $b_\alpha(G^k_{l^i}) \leq i \cdot b_\alpha(G^k_l)$ et $b_\delta(G^k_{l^i}) \leq \frac{l^i-1}{l-1} \cdot b_\delta(G^k_l)$.

Preuve. La preuve découle directement des équations de récurrences du lemme 1. Pour le nombre d'étapes, nous obtenons

$$\begin{aligned} b_\alpha(G^k_{l^i}) &\leq b_\alpha(G^k_l) + b_\alpha(G^k_{l^{i-1}}) \\ &\leq i \cdot b_\alpha(G^k_l) \end{aligned}$$

Pour la longueur des chemins, nous obtenons

$$\begin{aligned} b_\delta(G^k_{l^i}) &\leq l \cdot b_\delta(G^k_{l^{i-1}}) + b_\delta(G^k_l) \\ &\leq \frac{l^i-1}{l-1} \cdot b_\delta(G^k_l) \end{aligned}$$

□

Remarque 4 Lorsque l est impair, il est remarquable que du fait des équations de récurrence le rapport $\frac{b_\delta(G^k_{l^i})}{D(G^k_{l^i})}$ reste majoré par un rapport fixe égal à celui obtenu pour le premier tore, c'est-à-dire $\frac{b_\delta(G^k_l)}{D(G^k_l)}$.

Il ne reste plus qu'à initier correctement la récurrence. Pour cela il est nécessaire de trouver un bon protocole de diffusion dans les tores $TM(2k+1)^k$.

3. Diffusion dans le tore $TM(2k+1)^k$

3.1. *Propriétés requises*

Nous étudions dans cette partie les propriétés requises afin de diffuser en un nombre d'étapes optimal sur le tore $TM(2k+1)^k$. Nous supposons dorénavant que les éléments représentatifs de $\mathbb{Z}_{2k+1}$ sont $\{-k,\ldots,-1,0,1,\ldots,k\}$.

Notation 3 S_t *représente l'ensemble des sommets qui connaissent l'information* **après l'étape** t.

Dans le tore $TM(2k+1)^k$ le nombre potentiel minimum d'étapes est $\log_{2k+1}(2k+1)^k = k$. Effectuer une diffusion optimale en k étapes revient à chercher des ensembles S_t ayant les propriétés suivantes.

Propriétés 1

- $S_0 = \{0\}$ est le sommet émetteur,
- $S_k = \mathbb{Z}_{2k+1}^k$ est l'ensemble de tous les sommets du graphe,
- S_{t-1} peut prévenir S_t en une étape le long de chemins arc-disjoints.
- $|S_t| = (2k+1) \cdot |S_{t-1}|$,
- $S_{t-1} \subset S_t$,

Ces propriétés sont nécessaires et suffisantes. Notons que les deux dernières sont impliquées par les deux premières car le tore est de degré $2k+1$.

Nous introduisons à ce niveau une définition importante que nous détaillerons dans les sections suivantes.

Définition 3 *Les sommets S_{k-1} sont dit être les éléments d'un* **code parfait de rayon 1**, *s'ils vérifient la propriété suivante : chaque sommet de S_k est soit un élément de S_{k-1} soit un voisin direct (i.e. à distance 1) d'exactement un et un seul élément de S_{k-1}.*

Avant de décrire le protocole général de diffusion sur les tores de dimension k, nous redonnons brièvement le protocole optimal de Peters et Syska [PET 96], sur le tore de dimension 2, sous une forme nouvelle qui nous a permis de le généraliser. Nous appliquerons également cette méthode aux tores de dimension 3.

3.2. *Diffusion dans* $TM(5)^2$

Proposition 2 – (Peters, Syska [PET 96]) Il existe un protocole de diffusion dans le tore $TM(5)^2$ tel que $b_\alpha(TM(5)^2) = \log_5(5^2) = 2$ et $b_\delta(TM(5)^2) = D(TM(5)^2) = 4$.

Nous redonnons brièvement la preuve de cette proposition avec l'approche qui nous permettra de généraliser par la suite. Pour cela, nous définissons les ensembles S_t comme suit.

$$\begin{cases} S_2 &= \mathbb{Z}_5^2, \\ S_1 &= \{x \in S_2 \mid x_1 + 2x_2 = 0 \bmod 5\}, \\ S_0 &= \{0\}. \end{cases}$$

A partir de ces ensembles S_t il est facile de vérifier sur la figure 4 que les propriétés 1 sont vérifiées.

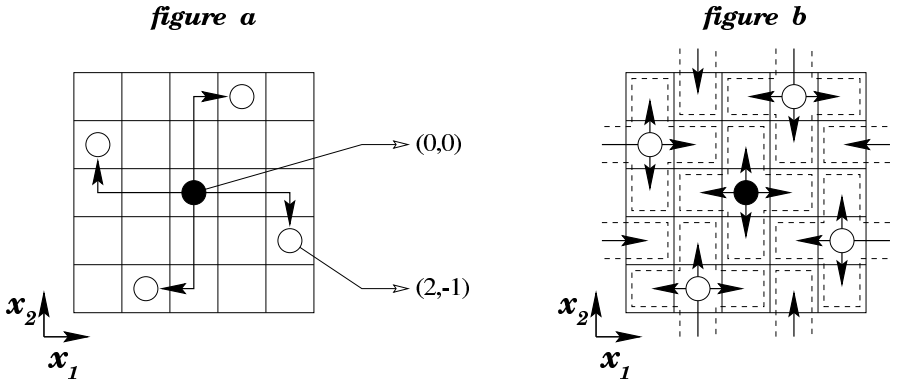

Fig 4 - *Les* `figures-a` *et* `b` *représentent le tore* $TM(5)^2$. *Le point central noir est le sommet émetteur* S_0, *c'est-à-dire le vecteur* 0. *L'ensemble des sommets noirs et du sommet blanc représente* S_1. *La* `figure-a` *montre que* S_0 *peut prévenir* S_1 *en une étape, le long de chemins arc-disjoints de longueur 3. La* `figure-b` *montre comment* S_1 *peut prévenir* S_2 *en une étape le long de chemins arc-disjoints de longueur 1.*

L'une des principales idées de cette méthode de diffusion est de remarquer que c'est à la dernière étape que rentre en jeu le plus grand nombre de communications. C'est donc à cette étape que la propriété "S_1 *informe* S_2 *le long de chemins arc-disjoints*" pourrait être la plus difficile à garantir. Mais cette propriété devient très facile à vérifier lorsque les sommets de S_1 sont pertinemment choisis de telle sorte que l'ensemble des sommets de S_1 et de leurs voisins directs forment l'ensemble des sommets de S_2 sans redondance. Cette propriété est vérifiée sur S_1 (Cf. figure 4-b). En fait, S_1 vérifie la définition 3 et est donc un code parfait.

3.3. *Diffusion dans* $TM(7)^3$

Proposition 3 – Il existe un protocole de diffusion dans le tore $TM(7)^3$ tel que $b_\alpha(TM(7)^3) = \log_7(7^3) = 3$ et $b_\delta(TM(7)^3) = \frac{10}{9}D(TM(7)^3)$.

Preuve. Comme sur le tore de dimension 2, nous commençons par définir les ensembles S_t.

$$\begin{cases} S_3 &= \mathbb{Z}_7^3, \\ S_2 &= \{x \in S_3 \mid x_1 + 2x_2 + 3x_3 = 0 \bmod 7\}, \\ S_1 &= \{x \in S_2 \mid x_1 + 3x_3 = 0 \bmod 7\}, \\ S_0 &= \{0\}. \end{cases}$$

A partir de ces définitions et des chemins indiqués sur la figure 5, on vérifie que les propriétés 1 sont satisfaites pour les deux premières étapes avec des chemins de longueur 5 et 4 respectivement.

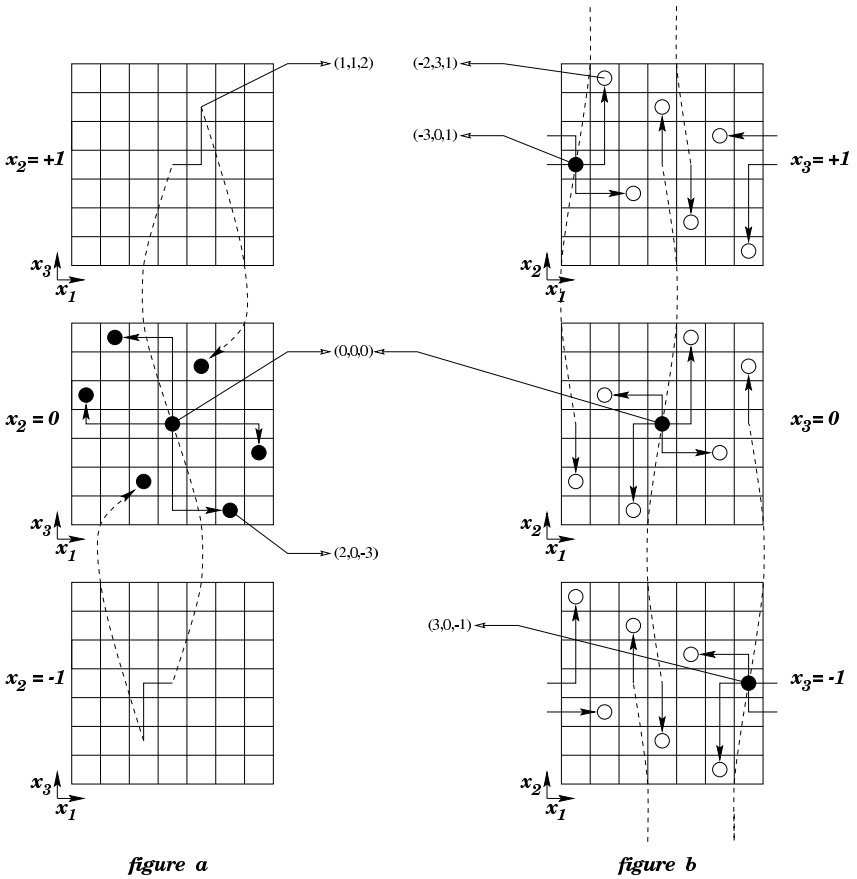

Fig 5 - *Schéma de diffusion dans le tore $TM(7)^3$. La* `figure-a` *représente la première étape de la diffusion. Le sommet central est le vecteur nul S_0. L'ensemble S_1 est représenté par les sommets noirs. Cette figure montre comment S_0 peut envoyer son information aux éléments de S_1 en utilisant des chemins arc-disjoints de longueur au plus 5. La* `figure-b` *décrit la deuxième étape de la diffusion. Les sommets blancs et noirs représentent les éléments de S_2. Cette figure montre le schéma de communication utilisé par les éléments de S_1 pour envoyer leur information sur les éléments de S_2. Chacun des 7 éléments de S_1 utilise les mêmes schémas de communications. Sur cette figure, seuls 3 des 7 éléments de S_1 sont représentés (en noir), néanmoins cela suffit pour remarquer que S_1 peut informer les éléments de S_2 le long de chemins arc-disjoints de longueur au plus 4.*

Ainsi, après cette deuxième étape, tous les sommets de S_2 ont été informés. Pour conclure le protocole par une dernière étape, il suffit de remarquer que S_2 est un code parfait. Ceci revient à dire que l'ensemble formé de chaque sommet de S_2 avec leurs voisins directs pave parfaitement le tore. La figure 6 représente un point de S_2 avec ses 6 voisins directs.

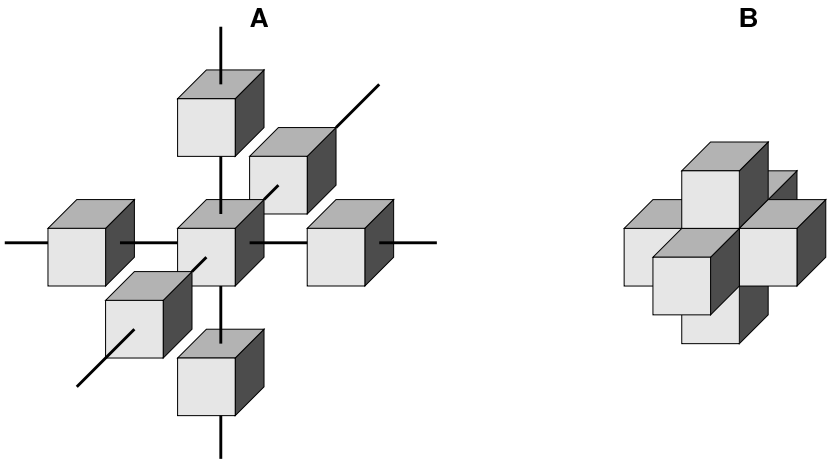

Fig 6 - *La* `figure-A` *représente un sommet de S_2 (ici au centre de la figure) relié à chacun de ses 6 voisins directs par un lien. Il en est de même pour la* `figure-B` *mais en omettant les liens. On peut voir cette* `figure-B`*, comme une structure de base en 3 dimensions. Il est possible d'emboîter 49 de ces structures pour former le tore $TM(7)^3$.*

Ainsi, la dernière étape s'effectue sans problème, puisque les sommets de S_2 n'ont plus qu'à envoyer leur information à chacun de leurs 6 voisins directs le long de chemins arc-disjoints de longueur 1. Le cœfficient $b_\delta(TM(7)^3)$ est donc égal à $5+4+1 = 10$. □

4. Généralisation de la diffusion dans $TM(2k+1)^k$

Afin de diffuser dans le tore $TM(2k+1)^k$, nous commençons comme précédemment par définir les ensembles S_t. Pour obtenir une diffusion en un nombre optimum d'étapes, il est nécessaire que $S_k = \mathbb{Z}^k_{2k+1}$. Nous chercherons ensuite à définir l'ensemble S_{k-1} à partir de la remarque suivante.

Dans un protocole de diffusion utilisant les ensembles S_t, l'étape dans laquelle est impliqué le plus grand nombre de communications est la dernière, c'est-à-dire lorsque les sommets de S_{k-1} informent ceux de S_k. Il est alors intéressant de choisir un ensemble S_{k-1} réparti de telle sorte que l'on sache réaliser aisément les communications de cette étape. C'est le cas si l'ensemble S_{k-1} vérifie la définition 3. En effet, si S_{k-1} est un code parfait de rayon 1, alors l'union des éléments de S_{k-1} et de tous leurs voisins directs correspond à S_k. La dernière étape se réduit alors à l'envoi par chaque sommets de S_{k-1} du message à chacun de ses voisins, les chemins sont alors tous de longueur 1 et clairement arc-disjoints.

Remarque 5 La distance dans le tore correspond à la distance de Lee sur $\mathbb{Z}^k_{2k+1}$ (voir [MCW 77]). La propriété que nous recherchons sur S_{k-1} se traduit en théorie des

codes ainsi : "*S_{k-1} est un code de Lee de rayon de recouvrement 1 de cardinalité $(2k+1)^{k-1}$, c'est donc un code parfait de rayon 1*".

De tels codes parfaits de rayon 1 sont bien connus, nous choisirons d'utiliser $S_{k-1} = \{x \in S_k \mid x_1 + 2x_2 + \cdots + kx_k = 0 \bmod (2k+1)\}$. Nous définissons alors les ensembles S_t inductivement comme suit : pour $k-1 \geq t \geq 1$, $S_{t-1} = \{x \in S_t \mid x_{t+1} = 0\}$. Les définitions des ensembles S_t se résument par :

$$\begin{cases} S_k & = & \mathbb{Z}_{2k+1}^k, \\ S_{k-1} & = & \{x \in S_k \mid \sum_{j=1}^{j=k} jx_j = 0 \bmod (2k+1)\}, \\ S_{t-1} & = & \{x \in S_t \mid x_{t+1} = 0\}, \text{ pour } k-1 \geq t \geq 1. \end{cases}$$

On peut facilement vérifier que les propriétés suivantes sont alors vraies : $S_0 = \{0\}$, $|S_t| = (2k+1) \cdot |S_{t-1}|$, et $S_{t-1} \subset S_t$. Pour que les ensembles S_t vérifient toutes les propriétés 1, il reste désormais à prouver que S_{t-1} peut informer S_t en une étape le long de chemins arc-disjoints. Nous le prouvons dans la proposition suivante et donnons en outre une borne supérieure relativement fine sur la longueur des chemins utilisés.

Proposition 4 – Pour $1 \leq t \leq k-1$, S_{t-1} peut informer S_t en une étape le long de chemins arc-disjoints de longueur au plus $k + 2 + \lceil \frac{k}{t} \rceil$.

Preuve. Tout d'abord, nous pouvons remarquer que S_t se partitionne en $2k+1$ classes que nous noterons $S_t(\alpha)$ avec $\alpha \in \mathbb{Z}_{2k+1}$ (les représentants étant pris là aussi dans $\{-k, \ldots, 0, \ldots, k\}$) définies par $S_t(\alpha) = \{x \in S_t \mid x_{t+1} = \alpha\}$. De fait, $S_t(\alpha)$ est l'intersection de S_t avec l'hyperplan défini par la condition $\{x_{t+1} = \alpha\}$. En particulier nous avons $S_t(0) = S_{t-1}$. Dans une première phase, $S_{t-1} = S_t(0)$ va informer, pour tout α, par une translation un ensemble de même cardinalité noté $U_t(\alpha)$ situé dans l'hyperplan $\{x_{t+1} = \alpha\}$. La deuxième phase consistera à translater en parallèle chaque $U_t(\alpha)$ sur $S_t(\alpha)$ au sein de l'hyperplan $\{x_{t+1} = \alpha\}$. A ce niveau, nous aurons besoin d'utiliser les $2k$ générateurs du tore. Ceux-ci sont définis comme les vecteurs e_i de dimension k tels que pour $1 \leq i \leq k$, $e_i = (0, \cdots, 0, +1, 0, \cdots, 0)$ a un $+1$ en $i^{ième}$ position, et $e_{-i} = -e_i$.

Pour réaliser la première phase nous utiliserons pour $\alpha \in \mathbb{Z}_{2k+1}$ les translations,

$$\begin{cases} x & \rightarrow & x + e_\alpha + \alpha e_{t+1} & \text{pour } \alpha \neq t+1 \text{ et } \alpha \neq -(t+1), \\ x & \rightarrow & x + (t+1)e_{t+1} & \text{pour } \alpha = t+1, \\ x & \rightarrow & x - (t+1)e_{t+1} & \text{pour } \alpha = -(t+1). \end{cases}$$

Les chemins associés sont 2 à 2 arc-disjoints, car pour un x donné on utilise des e_α distincts et que 2 sommets de S_{k-1} et donc a fortiori de $S_t(0)$, ne sont jamais adjacents.

Dans la seconde phase, rappelons que pour un α donné on travaille dans l'hyperplan satisfaisant la condition $\{x_{t+1} = \alpha\}$ et par conséquent il ne peut y avoir d'arcs en commun pour deux valeurs différentes de α. Pour un α fixé, il faut envoyer $U_t(\alpha)$ sur $S_t(\alpha)$. Comme $S_t(\alpha)$ est un translaté de $S_t(0)$, c'est aussi un translaté de $U_t(\alpha)$. Soit $w(\alpha)$ le vecteur de longueur minimale tel qu'il existe $z \in U_t(\alpha)$ et $x \in S_t(\alpha)$

avec $z + w(\alpha) = x$. Par linéarité nous avons donc $U_t(\alpha) + w(\alpha) = S_t(\alpha)$. On établit alors, depuis tout sommet de $U_t(\alpha)$ un chemin correspondant au vecteur $w(\alpha)$ obtenu par un routage utilisant les dimensions de $w(\alpha)$ dans un ordre fixé. Les chemins ainsi obtenus à partir de deux points distincts z et $y \in U_t(\alpha)$ respectivement vers $z + w(\alpha)$ et $y + w(\alpha)$, avec $z \neq y$, sont alors arc-disjoints. En effet, si un conflit apparaissait sur un arc uv, l'un des chemins zu ou yu serait strictement plus court que l'autre (dans le cas contraire, le routage étant fixé nous aurions $z = y$). Supposons qu'il s'agisse du chemin zu, alors le chemin $(zu), (uv), (v(y + w(\alpha)))$ serait strictement plus court que le chemin associé à $w(\alpha)$, ce qui contredirait la minimalité de $w(\alpha)$.

Afin de terminer la preuve, il nous reste à estimer la longueur des chemins utilisés. Dans la première phase, la longueur est au plus $|\alpha| + 1 \leq k + 1$. Dans la seconde phase, il faut majorer la longueur de $w(\alpha)$. Pour cela, nous allons exhiber une translation de $U_t(\alpha)$ vers $S_t(\alpha)$ tel que le chemin associé à la translation soit de longueur au plus $1 + \lceil \frac{k}{t} \rceil$, ce qui prouvera la proposition. Posons $f(x) = \sum_{j=1}^{j=k} j x_j$. Tout d'abord nous pouvons remarquer que si $x \in S_t(\alpha)$, alors $x_{t+1} = \alpha$, $x_{t+2} = \ldots = x_k = 0$ et $f(x) = 0$. Posons $V_t(\alpha) = U_t(\alpha) - e_\alpha$ pour $\alpha \neq \pm(t+1)$ et $V_t(\alpha) = U_t(\alpha)$ pour $\alpha = \pm(t+1)$. Alors si $x \in V_t(\alpha)$, on a aussi $x_{t+1} = \alpha$, $x_{t+2} = \ldots = x_k = 0$, mais cette fois-ci $f(x) = \alpha(t+1)$. Nous allons donc chercher une translation de $V_t(\alpha)$ sur $S_t(\alpha)$ qui n'utilise seulement que les t premières dimensions. Comme $-k \leq \alpha(t+1) \leq k$, posons $\alpha(t+1) = \epsilon p$, avec $0 \leq p \leq k$ et $\epsilon = +1$ si $0 < \alpha(t+1) \leq k$ et -1 sinon. Soit q et r tels que $p = qt + r$ avec $0 \leq r < t$. Alors $S_t(\alpha)$ peut être obtenu à partir de $V_t(\alpha)$ par la translation de vecteur $-(qe_{\epsilon t} + e_{\epsilon r})$. En effet, si $x \in V_t(\alpha)$, alors $f(x - (qe_{\epsilon t} + e_{\epsilon r})) = f(x) - (q\epsilon t + \epsilon r) = \epsilon p - (q\epsilon t + \epsilon r) = 0$. De plus comme $r < t$, les coordonnées en $t+1, t+2, \ldots, k$ n'ont pas changé. Donc le translaté de $x \in V_t(\alpha)$ est bien dans $S_t(\alpha)$. La longueur du chemin associé à la translation $-(qe_{\epsilon t} + e_{\epsilon r})$ est au plus $\lceil \frac{k}{t} \rceil$, car ou bien $r = 0$ et $q = \frac{p}{t} \leq \frac{k}{t}$ ou bien $r \neq 0$ et $q + 1 \leq \lceil \frac{p}{t} \rceil \leq \lceil \frac{k}{t} \rceil$. Donc la longueur du chemin entre $U_t(\alpha)$ et $S_t(\alpha)$ est majoré par $1 + \lceil \frac{k}{t} \rceil$ (le 1 correspond à la translation $-e_\alpha$ de $U_t(\alpha)$ sur $V_t(\alpha)$ lorsque $\alpha \neq \pm(t+1)$). □

Ainsi, nous sommes en mesure d'énoncer le corollaire suivant.

Corollaire 2 – Il existe un protocole de diffusion sur le tore $TM(2k+1)^k$ tel que $b_\alpha(TM(2k+1)^k) = \log_{2k+1}(2k+1)^k = k$ et $b_\delta(TM(2k+1)^k) < k(k + 3 + \ln(k-1)) - 2$.

Preuve. Il suffit de sommer, sur les $k-1$ premières étapes du protocole de diffusion, la majoration de la longueur des chemins obtenue en proposition 4 et de rajouter 1 pour la dernière étape (car S_{k-1} est un code parfait de rayon1). Ainsi, $b_\delta(TM(2k+1)^k) \leq k^2 + k - 2 + \sum_{t=1}^{t=k-1} \lceil \frac{k}{t} \rceil + 1$. Or, $\sum_{t=1}^{t=k-1} \lceil \frac{k}{t} \rceil \leq \sum_{t=1}^{t=k-1} (\frac{k}{t} + 1)$. Comme $\sum_{t=1}^{t=k-1} (\frac{k}{t} + 1) = 2k - 1 + k \sum_{t=2}^{t=k-1} \frac{1}{t} < 2k - 1 + k \int_1^{k-1} \frac{du}{u}$, alors, nous avons bien $2k - 1 + k \sum_{t=2}^{t=k-1} \frac{1}{t} < 2k - 1 + k \ln(k-1)$. □

Remarque 6 On peut améliorer la longueur des chemins dans la proposition 4 en définissant les translations de $S_t(0)$ dans $U_t(\alpha)$ pour $\alpha \neq \pm(t+1)$ par $x \to x + e_{\phi(\alpha)} +$

αe_{t+1} où $\phi(x)$ est une bijection de $\mathbb{Z}_{2k+1} - \{\pm(t+1)\}$ dans $\mathbb{Z}_{2k+1} - \{\pm(t+1)\}$. On peut alors choisir $\phi(\alpha)$ de manière à mieux minimiser la longueur d'un majorant de $w(\alpha)$. Une étude détaillée permet de ramener le cœfficient $b_\delta(TM(2k+1)^k)$ à $D(TM(2k+1)^k) + \sqrt{D(TM(2k+1)^k)}$.

5. Généralisation de la diffusion dans $TM((2k+1)^i)^k$

Dans les sections précédentes nous avons initié la récurrence en donnant des protocoles efficaces pour les tores $TM(2k+1)^k$. Il nous est désormais possible de fournir des protocoles efficaces pour les tores $TM((2k+1)^i)^k$. Nous pouvons ainsi établir le corollaire suivant.

Corollaire 3 – Il existe un protocole de diffusion dans le tore $TM((2k+1)^i)^k$ tel que $b_\alpha(TM((2k+1)^i)^k) = \log_{2k+1}((2k+1)^{i^k}) = ki$ et $b_\delta(TM((2k+1)^i)^k) \leq \frac{1}{k}(k+3+\ln(k-1)-\frac{2}{k})\cdot D(TM((2k+1)^i)^k)$. En particulier pour le tore de dimension 3 il existe un protocole de diffusion tel que $b_\alpha(TM(7^i)^3) = \log_7(7^{i^3}) = 3i$ et $b_\delta(TM(7^i)^3) = \frac{10}{9}D(TM(7^i)^3)$.

Preuve. La preuve découle directement des équations de récurrence de la proposition 1 et des valeurs particulières obtenues pour les tores $TM(2k+1)^k$ (notamment lorsque k=3) permettant d'initier la récurrence. □

6. Etude particulière pour le tore carré de dimension 4

Bien que l'étude précédente fournisse également un résultat pour le tore de dimension 4, nous montrons dans cette section, qu' il est possible d'obtenir, pour cette dimension, un algorithme optimal à la fois pour le nombre d'étapes et la longueurs des chemins.

L'étude de la diffusion sur le tore de dimension 4 devrait nous conduire à utiliser le tore $TM(9)^4$ contenant 6561 sommets. L'étude particulière de la diffusion sur ce tore apparaît bien entendu comme trop fastidieuse sur un si grand nombre de sommet, car il serait nécessaire d'exhiber les chemins arc-disjoints nécessaires à la réalisation de chacune des 4 étapes du protocole. Mais suite à une remarque de C. Delorme, l'étude devient triviale si l'on utilise le tore $TM(3)^4$ ne contenant lui que 81 sommets.

6.1. *Diffusion pour le tore* $TM(3)^4$

Ainsi, nous pouvons établir la proposition suivante.

Proposition 5 – Il existe un protocole de diffusion sur le tore $TM(3)^4$ tel que $b_\alpha(TM(3)^4) = \log_9(3^4) = 2$ et $b_\delta(TM(3)^4) = D(TM(3)^4)$.

Preuve. Nous commençons par définir la matrice M composée de 4 vecteurs colonnes appartenant chacun à $\mathbb{Z}_3^4$.

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & -1 \\ -1 & 1 & -1 & 0 \\ -1 & -1 & 0 & 1 \end{pmatrix}$$

Comme précédemment nous commençons par définir les ensembles S_t.

$$\begin{cases} S_2 = \mathbb{Z}_3^4, \\ S_1 = M \cup -M \cup \{0\}, \\ S_0 = \{0\}. \end{cases}$$

Les vecteurs du code S_1 sont les vecteurs colonnes des matrices M, $-M$ et du vecteur nul. Le lecteur pourra aisément vérifier que S_0 peut informer les 8 sommets de S_1 en une étape, le long de chemins arc-disjoints de longueur 3. La dernière étape ne pose pas de problème, car là encore il est facile de vérifier que S_1 forme un code parfait. Ainsi si chaque sommet de S_1 envoie son message à chacun de ces 8 voisins directs, alors S_1 informe S_2 le long de chemins arc-disjoints de longueur 1. □

Ce résultat résulte du fait que $M^2 = 0 \bmod 3$. Ainsi, la diffusion est optimale pour le nombre d'étapes et pour les longueurs des chemins.

6.2. *Généralisation de la diffusion pour le tore* $TM(9^i)^4$

En appliquant le résultat précédent à la proposition 1, nous sommes en mesure d'obtenir un protocole de diffusion optimum pour le nombre d'étapes et pour les longueurs des chemins sur les tore $TM(9^i)^4$.

Corollaire 4 – Il existe un protocole de diffusion dans le tore $TM(3^i)^4$ tel que $b_\alpha(TM(3^i)^4) = 2i$ et $b_\delta(TM(3^i)^k) = D(TM(3^i)^k)$.

Remarque 7 Comme le tore $TM(3^i)^4$ contient $3^{4i} = 9^{2i}$ sommets, alors le corollaire 4 implique l'optimalité de la diffusion sur le tore $TM(9^i)^4$.

Remerciements

Nous tenons à remercier J-C. Bermond, J. G. Peters ainsi que les arbitres pour leurs nombreux conseils et remarques utiles.

7. Références

[BAR 96] M. Barnett, D.G. Payne, R.A. van de Geijn, and J. Watts. « Broadcasting on Meshes with Wormhole Routing ». *Journal of Parallel and Distributed Computing*, 35(2): 111–122, June 1996.

[CAS] Jean de Casanice. « An overview of wormhole routing ». Laboratoire d'Informatique, Signaux et Systèmes de Sophia Antipolis CNRS URA 1376 - Equipe : *"Communication Algorithms at Sophia Antipolis - Nice"* (J-C. Bermond, E. Darrot, O. Delmas, E. Fleury, S. Perennes, M. Syska), En préparation.

[DEL 97] O. Delmas. « *Communications par commutation de circuits dans les réseaux d'interconnexion* ». Thèse de doctorat, Université de Nice - Sophia Antipolis, Laboratoire I3S-CNRS URA 1376, 1997.

[FEL 93] R. Feldmann, J. Hromkovic, S. Madhavapeddy, B. Monien, and P. Mysliwietz. « Optimal algorithms for dissemination of information in generalized communication modes ». Technical Report No. 115, Universität-Gesamthochschule-Paderborn, February 1993.

[FLE 96] E. Fleury. « *Communications, routage et architectures des machines à mémoire distribuée - Autour du routage wormhole* ». Thèse de doctorat, Université de Lyon, Ecole Normale Supérieure de Lyon, 1996.

[FRA 95] P. Fraigniaud. « *Vers un principe de localité pour les communications dans les réseaux d'interconnexion* ». Thèse d'habilitation, Université de Lyon, Laboratoire de l'Informatique du Parallèlisme - CNRS Ecole Normale Supérieure de Lyon, 1995.

[HO 95] C.T. Ho and M.Y. Kao. « Optimal broadcast in all-port wormhole-routed hypercube ». *IEEE Trans. on Parallel and Distributed Systems*, 6(2): 200–204, February 1995.

[KER 79] P. Kermani and L. Kleinrock. « Virtual cut-through: a new computer communication switching technique ». *Computers Networks*, 3: 267–286, 1979.

[KOD 96] T. Kodate. « *Communications stucturées dans les réseaux d'interconnexion* ». Thèse de doctorat, Université de Nice - Sophia Antipolis, Laboratoire d'Informatique, Signaux et Systèmes de Sophia Antipolis CNRS URA 1376, 1996.

[MCK 94] P. K. McKinley, Y-J. Tsai, and D. F Robinson. « A Survey of Collective Communication in Wormhole-Routed Massively Parallel Computers ». Technical Report MSU-CPS-95-35, Michigan State University, East Lansing, Michigan 48824, June 1994.

[MCW 77] F.J. McWilliams and N.J.A. Sloane. *The theory of Error-Correcting Codes*. North-Holland, 1977.

[NUG 88] S.F. Nugent. « The iPSC/2 direct-connect technology ». In G.C. Fox, editor, *Proceedings of 3rd Conference on Hypercube Concurrent Computers and Applications*, pages 51–60. ACM, 1988.

[PAR 94] J-Y. L. Park, S-K. Lee, and H-A. Choi. « Circuit-switched broadcasting in $d-$dimensional tori and meshes ». In *Proceedings Eighth Int'l Parallel Processing Symposium*, Cancun, Mexico, April 26-29 1994.

[PAR 96] J-Y. L. Park and H-A. Choi. « Circuit-switched broadcasting in torus and mesh networks ». *IEEE Trans. on parallel and distributed systems*, 7(2): 184–190, February 1996.

[PER 96] S. Perennes. « *Communications dans les réseaux d'interconnexion* ». Thèse de doctorat, Université de Nice - Sophia Antipolis, Laboratoire I3S-CNRS URA 1376, 1996.

[PET 96] J.G. Peters and M. Syska. « Circuit-Switched Broadcasting in Torus Networks ». *IEEE Trans. on Parallel and Distributed Systems*, 7(3), March 1996.

[RUM 94] Jean de Rumeur. *Communication dans les réseaux de processeurs*. Collection Etudes et Recherches en Informatique. Masson, Paris, 1994.

[SEI 90] C.L. Seitz. « Concurrent architectures ». In R. Suaya and G. Birtwist, editors, *VLSI and Parallel Computation*, pages 1–84. Morgan Kaufmann, 1990.

Circuit-switched gossiping in the 3-dimensional torus networks

Olivier Delmas, Stéphane Perennes*

Thème 1 — Réseaux et systèmes
Projet SLOOP

Rapport de recherche n ° ???? — Juillet 1996 — 21 pages

Abstract: in this paper we describe, in the case of short messages, an efficient gossiping algorithm for 3-dimensional torus networks (wrap-around or toroidal meshes) that uses synchronous circuit-switched routing. The algorithm is based on a recursive decomposition of a torus. The protocol requires an optimal number of rounds and a quasi-optimal number of intermediate switch settings to gossip in an $7^i \times 7^i \times 7^i$ torus.

Key-words: circuit-switching, gossiping, torus network, toroidal mesh, linear coding theory.

(Résumé : tsvp)

Version of January 6, 1997. A short version of this paper will appear in *Proceedings of the EuroPar'96 Conference* (Lyon - France - August 26-29, 1996)

* Email : {delmas, sp}@unice.fr

Unité de recherche INRIA Sophia Antipolis
2004 route des Lucioles, BP 93, 06902 SOPHIA ANTIPOLIS Cedex (France)
Téléphone : 04 93 65 77 77 – Télécopie : 04 93 65 77 65

Echange total en mode commutation de circuits dans les tores de dimension 3

Résumé : dans cet article nous décrivons, pour des messages courts, un algorithme d'échange total efficace dans les réseaux toriques (grilles toriques) de dimension 3 qui utilise un routage par commutation de circuits synchone. L'algorithme est basé sur une décomposition récursive du tore. Le protocole requiert un nombre d'étapes optimal et un nombre de commutateurs intermédiaires quasi-optimal pour diffuser dans le tore $7^i \times 7^i \times 7^i$.

Mots-clé : commutation de circuits, échange total, tore, grille torique, théorie des codes linéaires.

1 Introduction

We consider here algorithms on parallel or distributed memory multicomputer systems in which the processors communicate by exchanging messages over an interconnection network. We are interested in global (or structured) communication protocols as these protocols appear as basic routines in many applications for example in linear algebra [3, 4, 17] or in image processing [28]. Two basic protocols are broadcasting (a processor sends its message to all the other) and gossiping (in which a distinct message originated at each processor must be distributed to all the other processors). These algorithms strongly depend of the routing mechanism used and of the topology of the network (see [31]). We consider the "circuit-switched routing mode"; under this name we include the currently used mechanisms of routing like wormhole [32], virtual cut-through [22] or direct connect [29] routing. For example, the wormhole routing is used in the IBM SP2, the Intel Paragon or in the two last generations of Cray machines (T3D and T3E). With this kind of routing the efficiency of the protocol is less depending of the distance between processors than in the classical store and forward routing model. So simple and regular topologies like torus networks (or meshes) well adapted to numerical applications can be used. For example, the Cray T3D and T3E use a 3−dimensional torus structure. Our aim in this paper is to give an efficient gossiping algorithm under the circuit-switched mode in the 3−dimensional torus networks. Note that the same problem for the 2−dimensional torus networks was solved in [1] and other results on circuit-switched structured communications in torus can be found in [33].

This paper is organized as follows. In sections 1.1 to 1.4 we describe the different hypothesis used in this paper. Then in section 1.5 we give some definitions and notations before to establish in section 2 lower bounds for gossiping protocols in circuit-switched routing. In section 3 we will study the gossiping protocol in the 3−dimensional torus network. We give the protocol for the $7^i \times 7^i \times 7^i$ torus network. Note that we study the case of power of 7 because in our model this is the extremal case in terms of numbers of processors which can receive a message originating at one processor in a given number of rounds. The proof uses recursion and is based on a detailed study of the $7 \times 7 \times 7$ torus network. The number of rounds of the protocols matches the lower bound established in section 2. In the last part we discuss the case of large messages.

1.1 The circuit-switched model

In the circuit-switched mode, the principle is to establish between ordered pairs of nodes which must communicate, a "circuit" which will correspond to a dipath in the network between the source and the destination. As said before, this model regroup different kinds of routings like wormhole, virtual cut-through or direct connect routing. Although there exist important differences between these mechanisms (like acknowledgment, use of small or large intermediate buffer size, ...), these differences are too small and too difficult to analyze to be taken into account in a simple general modelization and to evaluate the performance of protocols. When any type of circuit-switched routing is used, and communication patterns

are arbitrary, deadlock is possible and many papers on wormhole routing are more concerned with deadlock avoidance than efficiency [5, 9, 10, 25, 26]. The most common deadlock avoidance method is the use of virtual channels which uses multiplexing to share physical links.

Here, in our "circuit-switched model", we will design a global protocol like a succession of rounds. During each round, there are communications between ordered pairs of nodes. In order to avoid blocking and loss of messages, we will suppose that during a given round the dipaths realizing the communications are pairwise arc-disjoint (note that some authors consider a stronger constraint as they ask for vertex-disjoint dipaths [11]). Moreover, we will suppose that our protocol is somewhat "synchronous", that is a round can start only when the communications of the precedings one are finished.

1.2 Communication time

In the "circuit-switched model" we will consider that the transmission time for a message of length L to be sent from a processor x to a processor y along a dipath of length l is $\alpha+l\delta+L\tau$ (linear cost model), where α is the time to initiate a new message transmission, δ is the time to switch an intermediate node, and $1/\tau$ is the bandwidth of the communications links. In most current machines, message transmissions are initiated in software and switching is done in hardware, so δ is usually much smaller than α. Furthermore, α is usually much larger than τ. In this paper we will suppose that the initial message length L is small. For long messages, one can use the pipelining techniques developed in the store and forward mode (for example see the survey [13]).

1.3 Network constraint

We will modelize our interconnection network by a symmetric digraph $G = (V(G), A(G))$, where the set $V(G)$ represent the processors and the set of arcs $A(G)$ the links between the processors (more exactly between the output and input buffers of the switches). We will use the link-bounded [13] (or shouting [15] or all-port or $\Delta-$port) model of communication in which a processor can use all of its communication links simultaneously. We also assume that the communication links are full-duplex so that messages can travel in both directions simultaneously. Furthermore, we assume that each node has an initial distinct message, but all these messages have the same small length L. Finally, we allow messages to be concatenated with negligible cost.

Within this model (when the goal is first to minimize the number of rounds), broadcasting has been studied for different networks like hypercube [18, 24], 2−dimensional torus [30], $k-$dimensional torus [7, 8] or Butterfly network [6]. For gossiping the problem is much harder and to our knowledge it has been studied only for hypercube [14] and 2−dimensional torus network [1].

1.4 Gossiping protocol

Let G be a symmetric digraph. Then in our circuit-switched model, we can define the cost of a gossiping protocol as:

Notation 1.1 The total time necessary to achieve a gossiping protocol *in a digraph G will be denoted by $g(G) = g_\alpha(G)\alpha + g_\delta(G)\delta + g_\tau(G)\tau$ where $g_\alpha(G)$ is the number of rounds of the protocol, $g_\delta(G)$ is the sum of the maximum communication distances of each ordered pairs of processors used in each round of the protocol and $g_\tau(G)$ is the flow of information.*

As said before, here we don't use pipeline techniques and consider only short messages (or equivalently suppose $\tau << \alpha$ and $\tau << \delta$). **So, we are mainly interested in determining the optimal $g_\alpha(G)$ and for an optimal $g_\alpha(G)$ we search to minimize the $g_\delta(G)$ parameter.**

For $g_\delta(G)$ a trivial lower-bound is the diameter $D(G)$. In section 2 we give a new non-trivial lower-bound for $g_\alpha(G)$.

1.5 Definitions

In this article, we will use the following definitions and notations.

- $\mathbb{Z}_q$ will denote the **additive group of integers modulo q.** In the following, when we use the set $\mathbb{Z}_{2k+1}$, the elements of this set will be taken in $\{-k, \ldots, -1, 0, 1, \ldots, k\}$.
- G will denote a **digraph** with vertex set $V(G)$ and arc set $A(G)$.
- N will denote the **number of vertices** of G, that is $N = |V(G)|$.
- $d_G(x, y)$ will denote the **distance** from a vertex $x \in V(G)$ to a vertex $y \in V(G)$ that is the length of the shortest dipath from x to y.
- $D(G)$ will denote the **diameter** of a digraph G, that is the maximum of the distances between every ordered pair of vertices: $D(G) = \max_{(x,y)\in V^2(G)} d_G(x, y)$.
- In a symmetric digraph G, $\Delta(G)$ (or Δ for short) will denote **maximum in-degree (or out-degree)** of G, that is the maximum over the in-degrees (or out-degrees) of all vertices $V(G)$.
- C_N will denote the symmetric directed cycle of order N.

Definition 1.2 *The* **cartesian sum** *(also called* **cartesian product** *or* **box product***) denoted by $G\Box G'$ of two digraphs $G = (V, A)$ and $G' = (V', A')$, is the digraph whose vertices are the ordered pairs (x, x') where x is a vertex of G and x' is a vertex of G'. The vertex (y, y') is a successor of the vertex (x, x') in $G\Box G'$ if and only $x = y$ and (x', y') is an arc of G', or if $x' = y'$ and (x, y) is an arc of G.*

Definition 1.3 The $k-$dimensional torus *is the cartesian sum of k symmetric directed cycles of orders $p_1, p_2, \ldots, p_k$ and is denoted by $TM(p_1, p_2, \ldots, p_k) = C_{p_1} \Box C_{p_2} \Box \cdots \Box C_{p_k}$.*

Remark 1.4 If all $p_i \geq 3$, $TM(p_1, p_2, \ldots, p_k)$ is a regular digraph of degree $\Delta = 2k$. Its order is $p_1 \times p_2 \times \cdots \times p_k$, the number of arcs is $2kN$ and its diameter is $\sum_{i=1}^{k} \lfloor \frac{p_i}{2} \rfloor$.

Notation 1.5 *When $p_1 = p_2 = \cdots = p_k$, we will use the abbreviated notation $TM(p)^k$ and suppose in what follows that $p \geq 3$.*

Remark 1.6 The $k-$dimensional torus is a vertex-transitive digraph where each vertex x of the $TM(p_1, p_2, \ldots, p_k)$ digraph can be seen as a k-tuple vector $(x_1, x_2, \ldots, x_k) \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}$. Each vertex $(x_1, x_2, \ldots, x_k)$ (or k-tuple vector) is joined by an arc to the $2k$ vertices (or k-tuple vectors) $(x_1, x_2, \ldots, x_i \pm 1, \ldots, x_k) \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_i} \times \cdots \times \mathbb{Z}_{p_k}$ for $1 \leq i \leq k$.

Definition 1.7 *A* **routing function** *R for a digraph G is a set of $N(N-1)$ dipaths $R = \{R(x,y) | x, y \in V(G)\}$, where $R(x,y)$ is a dipath in G from x to y.*

Definition 1.8 *Given a routing function R for the digraph G, the* **load of an arc** *$u \in A(G)$, denoted by $\pi(G, R, u)$, is the number of dipaths of R going through u.*

Definition 1.9 *Given a routing function R for the digraph G, the* **arc-forwarding index of** *(G, R), denoted by $\pi(G, R)$, is the maximum number of dipaths of R going through any arc of G, that is $\pi(G, R) = \max_{u \in A(G)} \pi(G, R, u)$.*

Definition 1.10 *The* **arc-forwarding index of the digraph** *G, denoted by $\pi(G)$, is defined as $\pi(G) = \min_R \pi(G, R)$.*

2 Lower bounds

We first give some additional definitions and notations.

Definition 2.1 *Given a gossip protocol in a digraph G, we will say that the ordered pair $(x, y) \in V(G) \times V(G)$* **uses the arc** *$u \in A(G)$* **at round** *$t$ if a message originated from x and finally reaching y goes through the arc u at round t of the gossip protocol.*

Definition 2.2 *Given a gossip protocol in a digraph G, the* **gossip load** *of an arc $u \in A(G)$ at round t denoted $\mathcal{GL}(u, t)$ is the number of couples $(x, y) \in V^2(G)$ using the arc u at round t of the gossip protocol.*

Definition 2.3 *Given a gossip protocol in a digraph G completed at round $g_\alpha(G)$, the* **total gossip load** *of an arc $u \in A(G)$ noted $\mathcal{TGL}(u)$ is defined as $\mathcal{TGL}(u) = \sum_{t=1}^{g_\alpha(G)} \mathcal{GL}(u, t)$.*

Proposition 2.4 *For a gossip protocol in a digraph G, there exists an arc u such that $\mathcal{TGL}(u) \geq \pi(G)$.*

Proof. Any gossip algorithm constructs at least a dipath from each vertex to each other one. By choosing for each ordered pair (x,y) one of these dipaths, we can associate with a gossip algorithm a routing R for the digraph G. For any dipath created from x to y by the gossip algorithm and for any arc u of the dipath there exists a round t such that the couple (x,y) uses the arc u at round t. Hence the total gossip load of any arc u is at least the load of u for the routing R. It remains to observe that there exists an arc of G whose load for the routing R is at least $\pi(G)$. □

Let G be a digraph of maximum degree Δ, we calculate an upper bound on the total gossip load of an arc $u \in A(G)$, for any gossip protocol with $g_\alpha(G)$ rounds.

Proposition 2.5 *Let G be a digraph with maximum degree Δ and order N. Let $t_0 = \lceil \log_{\Delta+1}(N) \rceil$. If $g_\alpha(G) \leq 2t_0$, then $\forall u \in A(G)$:*

$$\mathcal{TGL}(u) \leq N\left[\left(\frac{2}{\Delta} + 2t_0 - g_\alpha(G)\right)\cdot(\Delta+1)^{g_\alpha(G)-t_0} - \frac{2}{\Delta}\right]$$

Proof. The total gossip load of an arc u is the sum of the gossip load of u at round t for all the rounds $t \in \{1,\ldots,g_\alpha(G)\}$. At the end of the round $t-1$ a vertex knows at most $\mathcal{I}(t-1) = \min((\Delta+1)^{t-1}, N)$ pieces of information and so at round t at most $\min((\Delta+1)^{t-1}, N)$ pieces of information can go through arc u. After round t the information which has gone through u will be able to reach at most $\mathcal{I}(g_\alpha(G)-t) = \min((\Delta+1)^{g_\alpha(G)-t}, N)$ nodes. Hence the gossip load of u at round t cannot exceed $\mathcal{I}(t-1)\cdot\mathcal{I}(g_\alpha(G)-t) = \min((\Delta+1)^{t-1}, N)\cdot\min((\Delta+1)^{g_\alpha(G)-t}, N)$. So, as $(\Delta+1)^{t_0} \geq N$ and $(\Delta+1)^{t_0-1} < N$ (and we suppose that $g_\alpha(G) \leq 2t_0$, that is $g_\alpha(G) - t_0 \leq t_0$), we have the following array:

Round t	$\mathcal{I}(t-1)$	$\mathcal{I}(g_\alpha(G)-t)$	$\mathcal{GL}(u,t)$
$\{1,\ldots,g_\alpha(G)-t_0\}$	$(\Delta+1)^{t-1} < N$	$(\Delta+1)^{g_\alpha(G)-t} \geq N$	$N(\Delta+1)^{t-1}$
$\{g_\alpha(G)-t_0+1,\ldots,t_0\}$	$(\Delta+1)^{t-1} < N$	$(\Delta+1)^{g_\alpha(G)-t} < N$	$(\Delta+1)^{g_\alpha(G)-1}$
$\{t_0+1,\ldots,g_\alpha(G)\}$	$(\Delta+1)^{t-1} \geq N$	$(\Delta+1)^{g_\alpha(G)-t} < N$	$N(\Delta+1)^{g_\alpha(G)-t}$

Hence, the number of the dipaths on the arc u is:

$$\begin{aligned}
\mathcal{TGL}(u) &\leq N\sum_{i=0}^{g_\alpha(G)-t_0-1}(\Delta+1)^i + (2t_0-g_\alpha(G))(\Delta+1)^{g_\alpha(G)-1} + N\sum_{i=0}^{g_\alpha(G)-t_0-1}(\Delta+1)^i \\
&\leq 2N\sum_{i=0}^{g_\alpha(G)-t_0-1}(\Delta+1)^i + (2t_0-g_\alpha(G))(\Delta+1)^{g_\alpha(G)-1} \\
&\leq 2N\frac{(\Delta+1)^{g_\alpha(G)-t_0}-1}{\Delta} + (2t_0-g_\alpha(G))(\Delta+1)^{g_\alpha(G)-t_0}(\Delta+1)^{t_0-1}
\end{aligned}$$

as $(\Delta+1)^{t_0-1} < N$, we obtain:

$$\mathcal{TGL}(u) \leq N\left((\Delta+1)^{g_\alpha(G)-t_0}\left(\frac{2}{\Delta}+2t_0-g_\alpha(G)\right)-\frac{2}{\Delta}\right)$$

□

Consequently for any digraph we have the following theorem.

Theorem 2.6 *Let G be a digraph with maximum degree Δ and order N, and let $t_0 = \lceil \log_{\Delta+1}(N) \rceil$. If $g_\alpha(G) \leq 2t_0$ then*

$$g_\alpha(G) \geq t_0 + \log_{\Delta+1}\left(\frac{\pi(G)}{N}\right) - O\left(\log_{\Delta+1}\log_{\Delta+1} N\right)$$

Proof. By the proposition 2.4 we have,

$$\begin{aligned} N\left((\Delta+1)^{g_\alpha(G)-t_0}\left(\frac{2}{\Delta}+2t_0-g_\alpha(G)\right)-\frac{2}{\Delta}\right) &\geq \pi(G) \\ (\Delta+1)^{g_\alpha(G)-t_0}\left(\frac{2}{\Delta}+2t_0-g_\alpha(G)\right) &\geq \frac{\pi(G)}{N} \end{aligned}$$

When we take the logarithm in base $\Delta+1$ we obtain,

$$g_\alpha(G) - t_0 + \log_{\Delta+1}\left(\frac{2}{\Delta}+2t_0-g_\alpha(G)\right) \geq \log_{\Delta+1}\left(\frac{\pi(G)}{N}\right)$$

$$\begin{aligned} g_\alpha(G) &\geq t_0 + \log_{\Delta+1}\left(\frac{\pi(G)}{N}\right) - \log_{\Delta+1}\left(\frac{2}{\Delta}+2t_0-g_\alpha(G)\right) \\ &\geq t_0 + \log_{\Delta+1}\left(\frac{\pi(G)}{N}\right) - O\left(\log_{\Delta+1} t_0\right) \end{aligned}$$

□

In order to exploit the bound above we can use the lower bound on the arc-forwarding index.

Proposition 2.7 (M.C. Heydemann, J.C. Meyer, D. Sotteau [16]) *The arc-forwarding index for the $TM(n)^k$ symmetric digraph is $\pi(TM(n)^k) = \frac{n^k-1}{2}\lfloor\frac{n^2}{4}\rfloor$.*

Now, we are able to state the following corollary.

Corollary 2.8 *Given a gossip protocol in the $TM(n)^k$ digraph of degree $\Delta = 2k$, the number of rounds necessary to achieve this protocol is:*

$$g_\alpha(G) \geq (k+1)\log_{2k+1}(n) - O\left(\log_{2k+1}\log_{2k+1} n\right)$$

Proof. This corollary is correct as in [2, 7, 8] it has been shown that the total number of rounds to achieve a broadcasting (and the inverse as gathering) protocol in the $TM(n)^k$ digraph is t_0. Then a trivial gossiping protocol will be the concatenation of a gathering and a broadcasting protocol, so $g_\alpha(G) \leq 2t_0$. □

Remark 2.9 There exists a relationship between the arc-forwarding index and the vertex bisection, since in [23] R. Klasing established a lower bound of the same kind (in a model named two-way vertex-disjoint paths mode) by using vertex bisection width.

3 Gossiping in the 3-dimensional torus TM$(7^i)^3$

3.1 Case of TM$(7)^3$

Gossiping can be derived from the broadcast protocol given in [7, 8] and the forthcoming paper [2]. We will recall briefly the principle of this broadcast protocol. In the following, we will make use of the following notation and definitions.

- Here G denotes the $TM(7)^3$ symmetric digraph.
- According to remark 1.6 we will consider vertices of G as elements of the 3-dimensional vector-space $\mathbb{Z}_7^3$, with canonical base $\{e_1, e_2, e_3\}$. Vertex $(x_1e_1 + x_2e_2 + x_3e_3)$ will be denoted $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$.
- M will be a 3-dimensional matrix. For a given set U of vectors, MU will denote the image of U by M : $\{Mx \mid x \in U\}$.
- The sum of two sets of vectors U_1 and U_2 will be $U_1 + U_2 = \{x \mid x = u_1 + u_2, u_1 \in U_1, u_2 \in U_2\}$.

Definition 3.1 *$\mathcal{E}$ is the set of the 3-dimensional vector-space $\mathbb{Z}_7^3$ associated with all the vertices of G that is $\forall x \in V(G)$.*

Definition 3.2 *We will denote by $\mathcal{B}_1$ the set $\{e_1, e_2, e_3, 0, -e_1, -e_2, -e_3\}$.*

Remark 3.3 Note that $\mathcal{B}_1$ is the sphere of radius 1 centered on zero of $\mathbb{Z}_7^3$ for the Lee distance (see [27]). As $x + \mathcal{B}_1$ is the sphere of radius 1 centered on x, it also contains the neighbors of x in G union x (see figure 1).

Definition 3.4 *The* **code** *$\mathcal{C}$ is the set of vertices such that $\mathcal{C} = \{(x_1, x_2, x_3) \in \mathbb{Z}_7^3 | x_1 + 2x_2 + 3x_3 = 0\}$*

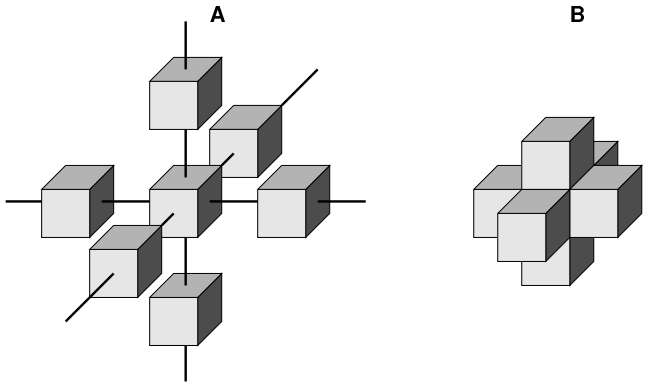

Figure 1: *A Lee sphere $\mathcal{B}_1$. Cubes represent vertices and the central cube is a vertex of the code $\mathcal{C}$ (see definition 3.4). On figure 1-A we represent the links (a link represents symmetric arcs) and on figure 1-B the representation without links. It's this pattern that we must pack to cover the entire torus (see remark 3.5).*

Remark 3.5 In coding theory [27], it is well known that $\mathcal{C}$ is a linear code of length 3 defined over $\mathbb{Z}_7$. Note that $\mathcal{C}$ has 49 elements like $(0,0,0),(-2,1,0),(2,-3,-1)$, and so on.

Definition 3.6 *Let* $M_0 = \begin{pmatrix} -2 & 0 & 1 \\ 1 & 2 & 3 \\ 0 & 1 & 0 \end{pmatrix}$ *and note that* $M_0^2 = \begin{pmatrix} -3 & 1 & -2 \\ 0 & 0 & 0 \\ 1 & 2 & 3 \end{pmatrix}$.

The broadcast algorithm relies on the following properties:

Property 3.7 $\mathcal{C} = M_0^2\mathcal{B}_1 + M_0\mathcal{B}_1$, and $\mathcal{E} = \mathcal{C} + \mathcal{B}_1$.

Proof. Just check the first equality. The second equation is well known in coding theory, because $\mathcal{C}$ is also a perfect Lee code [27]. □

Proposition 3.8 *There exists a gossiping protocol on the symmetric digraph $G = TM(7)^3$ with time $g(G) = 4\alpha + 12\delta + (1 + 7 + 7^2 + 7^3)L\tau$.*

To describe the gossiping protocol of proposition 3.8 we introduce some additional notation.

Notation 3.9 *Let x be a vertex of a digraph G and let $\mathcal{A} \subset V(G)$ be a subset of the set of vertices of G. The notation $x \to \mathcal{A}$* (resp. *$x \leftarrow \mathcal{A}$) is used when the vertex x sends his message towards all the vertices of $\mathcal{A}$* (resp. all the vertices of $\mathcal{A}$ send their own message toward the vertex *x).*

3.1.1 Description of the gossiping algorithm in $TM(7)^3$

The algorithm that we present here is similar to a method for designing so-called *"three-phase algorithms"* [19, 20, 21] (this method uses an accumulation, a gossip and a broadcast phase).

Begin *Gossiping Algorithm* *in* $TM(7)^3$.

All the information of the digraph G is concentrated (more exactly equally distributed) among the set of vertices of the code $\mathcal{C}$. This round uses dipaths of length 1 and messages of length L.

▷ **Round 1** ◁	
Concentration	
Scheme of communication	*Cost*
$\forall x \in \mathcal{C},\ x \leftarrow \{x + \mathcal{B}_1\}$	$\alpha + \delta + L\tau$

Here the scheme of communications is decomposed into two rounds. We will describe later the arc-disjoint dipaths used to perform these two rounds, and prove the cost of these rounds.

▷ **Step 2** ◁	
Gossiping among the vertices of $\mathcal{C}$	
Round 2-a	
Scheme of communication	*Cost*
$\forall x \in \mathcal{C},\ x \rightarrow \{x + M_0\mathcal{B}_1\}$	$\alpha + 5\delta + 7L\tau$
Round 2-b	
Scheme of communication	*Cost*
$\forall x \in \mathcal{C},\ x \rightarrow \{x + M_0^2\mathcal{B}_1\}$	$\alpha + 5\delta + 7^2L\tau$

Each vertex of the code $\mathcal{C}$ send its information to its 6 direct neighbors. This round uses dipaths of length 1 and messages of length 7^3L.

▷ **Round 3** ◁	
Final broadcasting	
Scheme of communication	*Cost*
$\forall x \in \mathcal{C},\ x \rightarrow \{x + \mathcal{B}_1\}$	$\alpha + \delta + 7^3L\tau$

End *Gossiping Algorithm* *in* $TM(7)^3$.

3.1.2 Analysis of the algorithm

- **Round 1:** As $\mathcal{C}$ is a perfect code, the first round equally distributes the entire information of G on the set of the vertices of $\mathcal{C}$.
- **Step 2:** During second step, each vertex $x \in \mathcal{C}$ has sent his information to $x + M_0\mathcal{B}_1 + M_0^2\mathcal{B}_1 = x + \mathcal{C} = \mathcal{C}$, thus step 2 performs a gossiping among the vertices of $\mathcal{C}$. Note that at the end of the round 1, vertices of $\mathcal{C}$ have a message of length $L_0 = 7L$. We will show in section 3.1.3 that rounds 2-a and 2-b use dipaths of length at most 5, hence step 2 is completed in time $(\alpha + 5\delta + L_0\tau) + (\alpha + 5\delta + 7L_0\tau)$.

  After step 2 each vertex x of $\mathcal{C}$ has received the whole information initially distributed on G.

- **Round 3:** As $\mathcal{E} = \mathcal{C} + \mathcal{B}_1$, this last round enables us to achieve the gossiping of the digraph.

3.1.3 Dipaths used by the algorithm

Now the problem is to exhibit a set of dipaths in G realizing each round of communication of the algorithm. As rounds 1 and 3 raise no problem, we give now the dipaths associated to step 2.

Round 2-a (resp. 2-b) uses communications of the kind $\forall x \in \mathcal{C}$, $x \to \{x + A\}$ (resp. $x \to \{x + A'\}$) with $A = M_0\mathcal{B}_1$ (resp. $A' = M_0^2\mathcal{B}_1$). In both cases, A and A' are symmetric, that is of the kind: $u_1, u_2, u_3, 0, -u_1, -u_2, -u_3$. We will describe for each u_i the dipath associated, the dipath associated to $-u_i$ being the opposite one. As there are many possible dipaths from x to $x + u_i$, we will describe them by decomposing the associated dipaths as $u_i = a_1 + a_2 + \ldots + a_l$, where a_i is proportional to some vector of the base, meaning that from x we first go to $x + a_1$ along vector a_1 then to $x + a_1 + a_2$ following a_2 and so on.

Dipaths used in the round 2-a In this case the vectors u_1, u_2, u_3 are

$$u_1 = \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} -2 \\ 0 \\ 0 \end{pmatrix}$$

$$u_2 = \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} + \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

$$u_3 = \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}$$

The maximum length of these dipaths is $\max(|+1|+|-2|; |-1|+|+2|+|+2|; |+1|+|+3|) = 5$ and the length of the messages is $7L$. Indeed after the first round each vertex $x \in \mathcal{C}$ has accumulated 7 pieces of information. The cost of this round is $\alpha + 5\delta + 7L\tau$. *Figure* 2-(2a) shows clearly that the scheme of communications described above is arc-contention free.

Dipaths used in the round 2-b In that case the vectors u_1, u_2, u_3 are

$$u_1 = \begin{pmatrix} -3 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -3 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

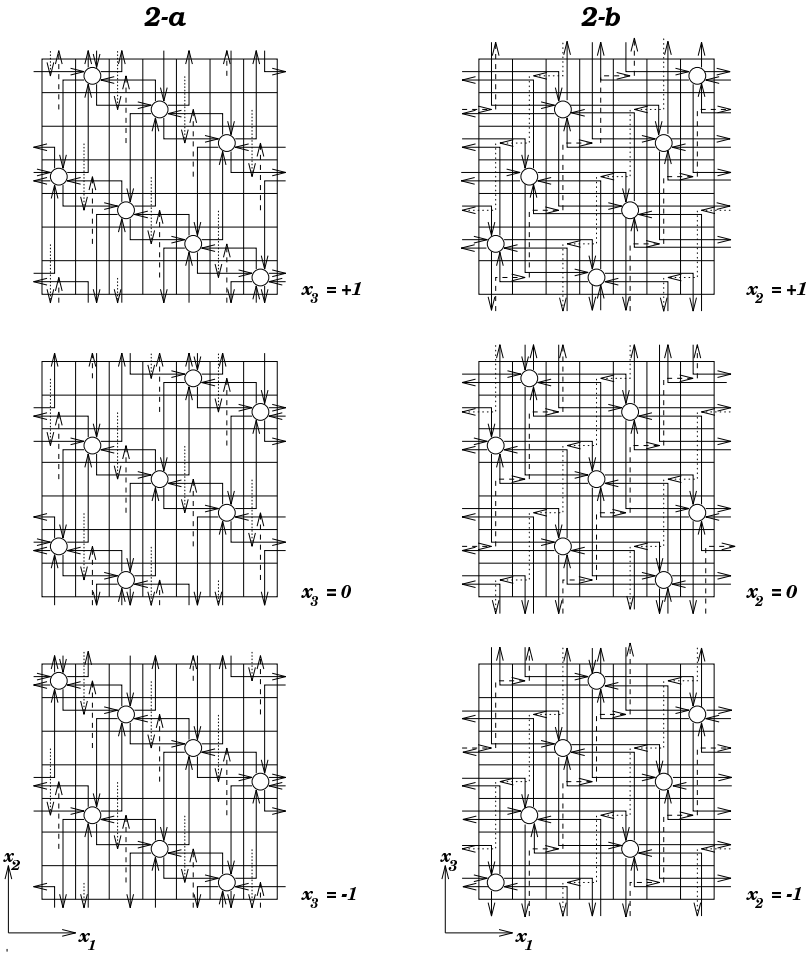

Figure 2: *Communication patterns for step 2 of the gossiping algorithm in the* $TM(7)^3$ *digraph. This step is decomposed into two rounds 2-a and 2-b. In the left* (resp. right) *drawing the torus is displayed with layers for a fixed* x_3 (resp. x_2). *Here, only three layers are displayed. In these figures the solid arcs correspond to the vectors* $u_1, -u_1, u_3, -u_3$, *the dashed arcs to vectors* u_2 *and the dotted arcs to vectors* $-u_2$ *for each round 2-a and 2-b.*

$$u_2 = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$u_3 = \begin{pmatrix} -2 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} + \begin{pmatrix} -2 \\ 0 \\ 0 \end{pmatrix}$$

The maximum length of the dipaths is $\max(|-3|+|+1|;|-1|+|+2|+|+1|+|+1|;|+3|+|-2|) = 5$ and the length of the messages is 7^2L. Indeed, after round 1 and 2-a each vertex of the code has 7×7 pieces of information. The cost of this round is $\alpha + 5\delta + 7^2L\tau$. *Figure* 2-(2b) shows clearly that the scheme of communications used in this round creates no-arc-contention.

3.2 Generalization for torus $TM(7^i)^3$

The main idea of this section is to use recursively the gossiping protocol designed for the torus $TM(7)^3$ in the torus $TM(7^i)^3$.

Notation 3.10 *Here G_i denotes the symmetric digraph $TM(7^i)^3$.*

Definition 3.11 *The* **code** *$\mathcal{C}_i$ is the set of the vertices of G_i defined as $\mathcal{C}_i = \{(x_1,x_2,x_3) \in \mathbb{Z}_{7^i}^3 | x_1 + 2x_2 + 3x_3 \equiv 0 \mod 7\}$.*

Remark 3.12 This code is once again a perfect code for the Lee distance [27]. Indeed, spheres of radius 1 centered on each vertex of the code $\mathcal{C}_i$ cover completely the digraph G_i. That is $V(G_i) = \mathbb{Z}_{7^i}^3 = \mathcal{B}_1 + \mathcal{C}_i$. The code $\mathcal{C}_i$ has 7^{3i-1} elements.

Notation 3.13 *Let U_0 be a sub-group of $\mathbb{Z}_{7^i}^3$ defined as $U_0 \equiv 0 \mod 7$.*

Remark 3.14 U_0 is clearly isomorphic to $\mathbb{Z}_{7^{i-1}}^3$. The sub-group U_0 which contains the vectors $x = (x_1,x_2,x_3)$ such that $x_1 \equiv 0 \mod 7$, $x_2 \equiv 0 \mod 7$ and $x_3 \equiv 0 \mod 7$, has $7^{i-1} \times 7^{i-1} \times 7^{i-1}$ vertices (or vectors).

Definition 3.15 *The* **family** *associated with a vector (or vertex) x is the set of vectors (or vertices) defined as $x + U_0$.*

Lemma 3.16 *In the $TM(7^i)^3$ symmetric digraph the vertices of the code $\mathcal{C}_i$ form 7^2 disjoint dilated sub-torus of the $TM(7^{i-1})^3$ symmetric digraph with a dilated factor of 7.*

Proof. The distance between two vertices of U_0 is a multiple of 7. If we join by a dipath of length 7 any ordered pair of vertices at distance exactly 7, we obtain a sub-graph H_0 of G_i which is a dilated sub-torus (obtained from the torus G_{i-1} by dilating each arc in a dipath of length 7). Now we can partition the vertices of the code $\mathcal{C}_i$ into 7^2 disjoint families. Indeed, any vertex (x_1,x_2,x_3) of the code $\mathcal{C}_i$ belongs to the family $(a,b,c) + U_0$ where $x_1 \equiv a \mod 7$, $x_2 \equiv b \mod 7$ and $x_3 \equiv c \mod 7$ with $-3 \leq a \leq 3$, $-3 \leq b \leq 3$ and $-3 \leq c \leq 3$. So, we have 7^2 possible choices for (a,b,c). Indeed, c is determined as soon as we fix a and b. If we consider the subgraph $H_{a,b}$ generated by the vertices of the family associated with (a,b,c), two vertices at distance 7 being joined by a dipath of length 7, $H_{a,b}$ is isomorphic to H_0, the dilated sub-torus of $TM(7^{i-1})^3$. Note that by definition any two different $H_{a,b}$ have no arc in common. So, we can in a given round, do concurrent communications on each $H_{a,b}$ (or families). □

Proposition 3.17 *There exists a gossiping protocol on the symmetric digraph* $G_i = TM(7^i)^3$ *with time* $g(G_i) = 4i\alpha + \frac{12}{9}D(G_i)\delta + [\frac{57}{49}(7^{i-1}-1) + \frac{7^3}{7^{2i}} - \frac{1}{7^{3i}}]\frac{NL}{6}\tau$.

We describe now the gossiping protocol of this proposition.

3.2.1 Description of the gossiping algorithm in $TM(7^i)^3$

Here the gossiping algorithm in $TM(7^i)^3$ is similar to gossiping algorithm in $TM(7)^3$.

Begin *Gossiping Algorithm* *in* $TM(7^i)^3$.

All the information of the digraph G_i is concentrated (more exactly equitably distributed) on the set of vertices of the code $\mathcal{C}_i$. This round uses dipaths of length 1 and messages of length L.

▷ **First Round Concentration** ◁	
Scheme of communication	*Cost*
$\forall x \in \mathcal{C}_i,\ x \leftarrow \{x + \mathcal{B}_1\}$	$\alpha + \delta + L\tau$

Vertices of the code $\mathcal{C}_i$ are partitioned into families. The vertices of the same family perform the gossiping protocol on the dilated subtorus $TM(7^{i-1})^3$ recursively. We will describe later the cost of this phase.

▷ **Recursive phase** ◁
Scheme of communication
Recursive gossiping protocol on G_{i-1}
Cost
$g_\alpha(G_{i-1})\alpha + 7g_\delta(G_{i-1})\delta + 7g_\tau(G_{i-1})L\tau$

For this step, the communications are similar to communications used in the step 2 of the gossiping protocol for the vertices of the code on $\mathbb{Z}_7^3$. At the beginning of this step the length of messages is $\frac{N}{7^2}L$.

▷ **Local Gossiping Step** ◁ **Gossiping between the vertices of** $\mathcal{C}_i$	
Round a	
Scheme of communication	*Cost*
$\forall x \in \mathcal{C}_i,\ x \rightarrow \{x + M_0\mathcal{B}_1\}$	$\alpha + 5\delta + \frac{N}{7^2}L\tau$
Round b	
Scheme of communication	*Cost*
$\forall x \in \mathcal{C}_i,\ x \rightarrow \{x + M_0^2\mathcal{B}_1\}$	$\alpha + 5\delta + \frac{N}{7}L\tau$

Each vertex of the code $\mathcal{C}_i$ sends its information to its 6 direct neighbors. This round uses dipaths of length 1 and messages of length NL.

▷ **Last Round Final broadcasting** ◁	
Scheme of communication	*Cost*
$\forall x \in \mathcal{C}_i,\ x \rightarrow \{x + \mathcal{B}_1\}$	$\alpha + \delta + NL\tau$

End *Gossiping Algorithm* *in* $TM(7^i)^3$.

3.2.2 Analysis of the algorithm and recursion

- The **first round** raises no problem.
- At the beginning of the **recursive phase** the length of messages is $7L$. As this phase performs a gossiping protocol on the dilated sub-torus G_{i-1}, then the distances of the communications have a dilation factor of 7 and this recursive phase can be applied on each family in a same partition in the same time because these families are disjoint.
- As this **local gossiping step** used the same scheme of communication as step 2 on $TM(7)^3$, then each vertex of a family receives information from a vertex of each other family. So, the cost of this step is $(\alpha + 5\delta + \frac{N}{7^2}L\tau) + (\alpha + 5\delta + 7\frac{N}{7^2}L\tau)$.
- This **last step** raises no problem. Just note that at this step each vertex of the code $\mathcal{C}_i$ knows all the information of G_i, so the length of the messages is $7^{3i}L$.

From this algorithm and recursion we obtain (with $N = 7^{3i}$),

$$\begin{array}{lcll} g_\alpha(G_i) & = & g_\alpha(G_{i-1}) + 4 & = & 4i \\ g_\delta(G_i) & = & 7g_\delta(G_{i-1}) + 12 & = & \frac{12}{9}D(G_i) \\ g_\tau(G_i) & = & 7g_\tau(G_{i-1}) + 1 + (1 + \frac{1}{7} + \frac{1}{7^2})N & = & [\frac{57}{49}(7^{i-1} - 1) + \frac{7^3}{7^{2i}} - \frac{1}{7^{3i}}]\frac{N}{6} \end{array}$$

4 Case of large messages

In the previous parts we presented the case for short messages as we focused only on the parameters $\alpha(G)$ and $\delta(G)$. But our protocols are not efficient if we consider large messages. Indeed the predominant parameter becomes $\tau(G)$. Our previous algorithms imply a maximal parameter $\tau(G)$ at the last round (final broadcasting). In this part we discuss the case of large messages and will show that it is possible to decrease the parameter $\tau(G)$ using classical methods, if we allow an increase in the parameter $\alpha(G)$ (see [1]). Here we use the following definition and lemma.

Definition 4.1 *Let x be a vertex (or vector) of the $TM(7^i)^3$ symmetric digraph, and let $c(x)$ denote the color of the vertex x defined by $c(x) = (x_1 + 2x_2 + 3x_3) \mod 7$, so $c(x) \in \Omega = \{-3, -2, -1, 0, 1, 2, 3\}$.*

Lemma 4.2 *The vertices of the $TM(7^i)^3$ digraph can be partitioned with 7 different colors such that a vertex x and its direct neighbors all have different colors.*

Proof. Just use the $c(x)$ colors and note that the direct neighbors of the vertex x are the vertices with ± 1 on only one coordinate x_1 or x_2 or x_3. Thus x and its direct neighbors all have different values. □

4.1 Case of $TM(7)^3$

As we saw in section 3.1, at the beginning of the last round (final broadcasting) of the gossiping protocol on the symmetric digraph $G = TM(7)^3$, all the vertices of the code $\mathcal{C}$ know the entire information of G. During this last round each vertex of the code sends the total information to its direct neighbors using its out-links (out-arcs) and no out-arc of the vertices which are not in the code are used. The idea is to split this last round into two using out-arcs of the vertices which are not in the code to decrease the data flow on the out-arcs of the vertices in the code by involving smaller messages.

Proposition 4.3 *There exists a gossiping protocol on the symmetric digraph $G = TM(7)^3$ with time $g(G) = 5\alpha + 13\delta + (1 + 7 + 3 \cdot 7^2)L\tau$.*

Proof. We split the last round (final broadcasting) into two.

Just before step 3, the message is splitted into 7 pieces and during rounds 3-a and 3-b the vertices of the code send a different piece of the total message (that is $1/7th$ of the total length of the initial message) to each neighbor. During round 3-b the vertices which are not in the code send the message they have received at round 3-a toward their direct neighbors.

▷ **Step 3** **Final broadcasting** ◁	
Round 3-a	
Scheme of communication	*Cost*
$\forall x \in \mathcal{C}, x \xrightarrow{\frac{1}{7}} \{x + \mathcal{B}_1\}$	$\alpha + \delta + \frac{7^3}{7}L\tau$
Round 3-b	
Scheme of communication	*Cost*
$\forall x \in \mathcal{C}, x \xrightarrow{\frac{1}{7}} \{x + \mathcal{B}_1\}$ and $\forall x \notin \mathcal{C}, x \rightarrow \{x + \mathcal{B}_1\}$	$\alpha + \delta + \frac{7^3}{7}L\tau$

At the beginning of round 3-a, all the vertices of the code $\mathcal{C}$ which know the entire information of G, partition their total message m of length 7^3 into 7 pieces (as for the concatenation, we forget the time necessary to partition the message). Now we give a different color from the set Ω to each piece of the message and we will denote each one by its color, that is $m = m_{-3}, m_{-2}, \cdots, m_2, m_3$ (this operation is exactly the same for all the vertices of the code). Then, during step 3-a each vertex of the code sends the piece of message m_i to y $\forall y \in \{x + \mathcal{B}_1\}$ if and only if $c(y) = i$. So, at the end of this round, the vertex x, $\forall x \notin \mathcal{C}$, knows the piece of message $m_{c(x)}$.

Now, lemma 4.2 assure that round 3-b achieves the gossiping protocol. Just note that during this last round the vertices of the code send the piece of message m_0. □

4.2 Case of $TM(7^i)^3$

Now we are able to state the generalization for the symmetric digraph $G_i = TM(7^i)^3$.

Proposition 4.4 *There exists a gossiping protocol on the symmetric digraph $G_i = TM(7^i)^3$ with time $g(G_i) = 5i\alpha + \frac{13}{9}D(G_i)\delta + [\frac{22}{49}(7^{i-1} - 1) + \frac{19 \cdot 7}{7^{2i}} - \frac{1}{7^{3i}}]\frac{NL}{6}\tau$.*

Proof. As the lemma 4.2 is true for G_i, just split the last round of each recursive phase and the last round (final broadcasting) of the gossiping protocol in $TM(7^i)^3$ by the 2 rounds described in the proof of proposition 4.3. □

Remark 4.5 If we are not concerned by the $g_\alpha(G)$ parameter, it is possible to decrease the data flow much more, as we can simulate the store-and-forward model with the wormhole model. Such technics in the store-and-forward model are described in the survey [13] and P. Fraignaud presents in [12] a protocol which decreases significantly the data flow as he obtains for the graph $TM(p)^k$ of order N, $g(TM(p)^k) \leq k\lfloor\frac{p}{2}\rfloor(\alpha+\delta) + \frac{(N-1)}{2k}\tau$.

Acknowledgments

The authors are grateful to J-C. Bermond, J. G. Peters and M. Syska for helpful discussions and remarks.

References

[1] C. Calvin, S. Perennes, and D. Trystram. Gossiping in torus with wormhole-like routing. In *7-th IEEE Symposium on Parallel and Distributed Processing (SPDP '95)*, San Antonio, USA, October 1995.

[2] Jean de Casanice. An overview of wormhole routing. Laboratoire d'Informatique, Signaux et Systèmes de Sophia Antipolis CNRS URA 1376 - Equipe : *"Communication Algorithms at Sophia Antipolis - Nice"* (J-C. Bermond, E. Darrot, O. Delmas, E. Fleury, S. Perennes, M. Syska), En préparation.

[3] M. Cosnard and P. Fraigniaud. Finding the roots of a polynomial on an mimd multicomputer. *Parallel Computing*, 15:75–85, 1990.

[4] M. Cosnard and D. Trystram. *Algorithmes et architectures parallèles.* Informatique Intelligence Artificielle. InterEditions, 1993.

[5] W.J. Dally and C.L. Seitz. Deadlock-free message routing in multiprocessor interconnection networks. *IEEE Transsaction on Computers*, C-36(5):547–553, May 1987.

[6] O. Delmas. *Communications par commutation de circuits dans les réseaux d'interconnexion.* Thèse de doctorat, Université de Nice - Sophia Antipolis, Laboratoire I3S-CNRS URA 1376, 1997.

[7] O. Delmas and S. Perennes. Diffusion en mode commutation de circuits. In R. Castanet and J. Roman, editors, *Proceedings of the 8th RenPar Conference*, pages 53–56, Bordeaux, France, May 1996.

[8] O. Delmas and S. Perennes. Diffusion en mode commutation de circuits dans les tores de dimension k. Laboratoire I3S - CNRS URA 1376 - Accepté avec révisions à la revue Technique et Science Informatiques. Hermès, AFCET, Paris., 1996.

[9] J. Duato. A necessary and sufficient condition for deadlock-free adaptive routing in wormhole networks. *IEEE Transactions on Parallel and Distributed Systems*, 6(10), October 1995.

[10] J. Duato. A theory of deadlock-free adaptive multicast routing in wormhole networks. *IEEE Transactions on Parallel and Distributed Systems*, 6(9), September 1995.

[11] R. Feldmann, J. Hromkovic, S. Madhavapeddy, B. Monien, and P. Mysliwietz. Optimal algorithms for dissemination of information in generalized communication modes. Technical Report No. 115, Universität-Gesamthochschule-Paderborn, February 1993.

[12] P. Fraigniaud. *Communications intensives dans les architectures à mémoire distribuée et algorithmes parallèles pour la recherche de racines de polynômes.* Thèse de doctorat, Université de Lyon I, E.N.S.L, 1990.

[13] P. Fraigniaud and E. Lazard. Methods and problems of communication in usual networks. *Discrete Applied Mathematics*, 53:79–133, 1994. Special volume proceedings international workshop on broadcasting and gossiping 1990.

[14] S. Fujita and M. Yamashita. Optimal group gossiping in hypercubes under a circuit-switching model. *SIAM Journal on Computing*, 25(5):1045–1060, October 1996.

[15] S.M. Hedetniemi, S.T. Hedetniemi, and A.L. Liestman. A survey of gossiping and broadcasting in communication networks. *Networks*, 18:319–349, 1986.

[16] M-C. Heydemann, J-C. Meyer, and D. Sotteau. On forwarding indices of networks. *Discrete Applied Mathematics*, 23:103–123, 1989.

[17] C.T. Ho and S.L. Johnsson. Optimum broadcasting and personalized communication in hypercubes. *IEEE Transactions on Computers*, 38(9):1249–1268, 1989.

[18] C.T. Ho and M.Y. Kao. Optimal broadcast in all-port wormhole-routed hypercube. *IEEE Transactions on Parallel and Distributed Systems*, 6(2):200–204, February 1995.

[19] J. Hromkovič, R. Klasing, and E.A. Stöhr. Gossiping in vertex-disjoint paths mode in interconnection networks. In Springer Verlag, editor, *Proc. 19th Int. Workshop on Graph-Theoretic Concepts in Computer Science (WG'93)*. LNCS, 1993. to appear.

[20] J. Hromkovič, R. Klasing, E.A. Stöhr, and H. Wagener. Gossiping in vertex-disjoint paths mode in $d-$dimensional grids and planar graphs. In Springer Verlag, editor, *Proc. First Annual European Symposium on Algorithms (ESA'93)*, pages 200–211. LNCS 726, 1993.

[21] J. Hromkovič, R. Klasing, W. Unger, and H. Wagener. Optimal algorithms for broadcast and gossip in the edge-disjoint paths modes. In Springer Verlag, editor, *Proc. 4th Scandinavian Workshop on Algorithm Theory (SWAT'94)*. LNCS, 1994. to appear.

[22] P. Kermani and L. Kleinrock. Virtual cut-through: a new computer communication switching technique. *Computers Networks*, 3:267–286, 1979.

[23] R. Klasing. The relationship between gossiping in vertex-disjoint paths mode and bisection width. In *Proc. 19th Int. Symp. on Mathematical Foundations of Computer Science*, 1994.

[24] T. Kodate. *Communications stucturées dans les réseaux d'interconnexion.* Thèse de doctorat, Université de Nice - Sophia Antipolis, Laboratoire d'Informatique, Signaux et Systèmes de Sophia Antipolis CNRS URA 1376, 1996.

[25] X. Lin, P.K. McKinley, and A-H. Esfahanian. Adaptative multicast wormhole routing in 2D mesh multicomputers. *Journal of Parallel and Distributed Computing*, 28(1):19–31, July 1995.

[26] D.H. Linder and J.C. Harden. An adaptive and fault tolerant wormhole routing strategy for $k-$ary $n-$cubes. *IEEE Trans. Computers*, 40(1):2–12, January 1991.

[27] F.J. McWilliams and N.J.A. Sloane. *The theory of Error-Correcting Codes.* North-Holland, 1977.

[28] S. Miguet. *Programmation dynamique et traitement d'images sur machines parallèles à mémoire distribuée.* PhD thesis, Université de Lyon, Ecole Normale Supérieure de Lyon, 1990.

[29] S.F. Nugent. The iPSC/2 direct-connect technology. In G.C. Fox, editor, *Proceedings of 3rd Conference on Hypercube Concurrent Computers and Applications*, pages 51–60. ACM, 1988.

[30] J.G. Peters and M. Syska. Circuit-Switched Broadcasting in Torus Networks. *IEEE Transactions on Parallel and Distributed Systems*, 7(3), March 1996.

[31] Jean de Rumeur. *Communication dans les réseaux de processeurs.* Collection Etudes et Recherches en Informatique. Masson, Paris, 1994.

[32] C.L. Seitz. Concurrent architectures. In R. Suaya and G. Birtwist, editors, *VLSI and Parallel Computation*, pages 1–84. Morgan Kaufmann, 1990.

[33] C. Spencer. *Circuit-switched structured communications on toroidal meshes.* PhD thesis, Simon Fraser University, February 1994.

Contents

Hamilton circuits in the directed Butterfly network

Jean-Claude Bermond, Eric Darrot, Olivier Delmas, Stéphane Perennes*

Thème 1 — Réseaux et systèmes
Projet SLOOP

Rapport de recherche n°???? — Juillet 1996 — 25 pages

Abstract: in this paper, we prove that the wrapped Butterfly digraph $\vec{\mathcal{WBF}}(d,n)$ of degree d and dimension n contains at least $d-1$ arc-disjoint Hamilton circuits, answering a conjecture of D. Barth. We also conjecture that $\vec{\mathcal{WBF}}(d,n)$ can be decomposed into d Hamilton circuits, except for $\{d=2$ and $n=2\}$, $\{d=2$ and $n=3\}$ and $\{d=3$ and $n=2\}$. We show that it suffices to prove the conjecture for d prime and $n=2$. Then, we give such a Hamilton decomposition for all primes less than 12000 by a clever computer search, and so, as corollary, we have a Hamilton decomposition of $\vec{\mathcal{WBF}}(d,n)$ for any d divisible by a number q, with $4 \leq q \leq 12000$.

Key-words: Butterfly graph, graph theory, Hamilton decomposition, Hamilton cycle, Hamilton circuit, perfect matching.

(Résumé : tsvp)

This work has been supported by the CEFIPRA (French-Indian collaboration) and the European project HCM MAP.

Version of January 12, 1997 submitted to DISCRETE APPLIED MATHEMATICS.

* Email : {bermond, darrot, delmas, sp}@unice.fr

Unité de recherche INRIA Sophia Antipolis
2004 route des Lucioles, BP 93, 06902 SOPHIA ANTIPOLIS Cedex (France)
Téléphone : 04 93 65 77 77 – Télécopie : 04 93 65 77 65

Circuits Hamiltoniens dans le réseau Butterfly orienté

Résumé : dans cet article, nous prouvons que le graphe Butterfly rebouclé (dans sa version orienté) $\mathcal{WB}\mathcal{F}(d,n)$ de degré d et de dimension n contient au moins $d-1$ circuits Hamiltoniens arc-disjoints, répondant à une conjecture de D. Barth. Nous conjecturons aussi que $\mathcal{WB}\mathcal{F}(d,n)$ peut être décomposé en d circuits Hamiltoniens, sauf pour $\{d=2$ et $n=2\}$, $\{d=2$ et $n=3\}$ et $\{d=3$ et $n=2\}$. Nous montrons qu'il suffit de prouver cette conjecture pour d premier et $n=2$. Puis nous donnons une telle décomposition pour tous les premiers jusqu'à 12000 grâce à une subtilité de programmation, induisant comme corollaire que $\mathcal{WB}\mathcal{F}(d,n)$ admet une décomposition Hamiltonienne pour tout d divisible par un nombre q tel que $4 \leq q \leq 12000$.

Mots-clé : Graphe Butterfly, Théorie des graphes, décomposition Hamiltonienne, cycle Hamiltonien, circuit Hamiltonien, couplage parfait.

1 Introduction and notations

1.1 Butterfly networks

Many interconnection networks have been proposed as suitable topologies for parallel computers. Among them the *Butterfly networks* have received particular attention, due to their interesting structure.

First, we have to warn the reader that under the name *Butterfly* and with the same notation, different networks are described. Indeed, if some authors consider the *Butterfly networks* as multistage networks used to route permutations, others consider them as point-to-point networks. In what follows, we will call the multistage version *Butterfly* and we will use Leigthon's terminology [13], namely *wrapped Butterfly*, for the point-to-point version. Furthermore, these networks can be considered either as undirected or directed. To be complete, we recall that some authors consider only *binary Butterfly networks* that is the restricted class of networks obtained when the out-degree is 2 (directed case) or 4 (undirected case).

In this article, we will use the following definitions and notation. $\mathbb{Z}_q$ will denote the set of integers modulo q. (For definitions not given here see [15]).

Definition 1.1 *The* **Butterfly digraph** *of degree d and dimension n, denoted $\vec{\mathcal{BF}}(d,n)$ has as vertices the ordered pairs (x,l), where x is an element of $\mathbb{Z}_d^n$ that is a word $x_{n-1}x_{n-2}\cdots x_1x_0$ where the letters belong to $\mathbb{Z}_d$ and $0 \leq l \leq n$ (l is called the level). For $l < n$, a vertex $(x_{n-1}x_{n-2}\cdots x_1x_0, l)$ is joined by an arc to the d vertices $(x_{n-1}\cdots x_{l+1}, \alpha, x_{l-1}\cdots x_0, l+1)$ where α is any element of $\mathbb{Z}_d$.*

$\vec{\mathcal{BF}}(d,n)$ has $(n+1)d^n$ vertices. Each vertex in level $l < n$ has out-degree d. This digraph is not strongly connected. It is mainly used as a multistage interconnection network (the levels corresponding to the stages) in order to route some one-to-one mapping of d^n inputs (nodes at level 0) to d^n outputs (nodes at level n).

The underlying undirected graph obtained by forgetting the orientation will be denoted $\mathcal{BF}(d,n)$.

Figure (**1**) shows simultaneously $\mathcal{BF}(3,2)$ and $\vec{\mathcal{BF}}(3,2)$. The orientation on $\vec{\mathcal{BF}}(d,n)$ being obtained by directing the edges from left to right.

Note that $\vec{\mathcal{BF}}(d,n)$ is often represented (for example in [13, 15]) in an opposite way to our drawing as the authors denote the nodes $(x_0x_1\cdots x_{n-1})$. We have chosen the representation which emphasizes the most on the recursive decomposition of $\vec{\mathcal{BF}}(d,n)$ and provides us an easy representation of our inductive construction (see section 3).

Definition 1.2 *The* **wrapped Butterfly digraph** *$\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ is obtained from $\vec{\mathcal{BF}}(d,n)$ by identifying the vertices of the last and first level namely (x,n) with $(x,0)$. In other words the vertices are the ordered pairs (x,l) where x is an element of $\mathbb{Z}_d^n$ that is a word $x_{n-1}x_{n-2}\cdots x_1x_0$ where the letters belong to $\mathbb{Z}_d$ and $l \in \mathbb{Z}_n$ (l is called the level). For any l, a vertex $(x_{n-1}x_{n-2}\cdots x_1x_0, l)$ is joined by an arc to the d vertices $(x_{n-1}\cdots x_{l+1}, \alpha, x_{l-1}\cdots x_0,\ l+1)$ where α is any element of $\mathbb{Z}_d$ (and where $l+1$ has to be taken modulo n).*

Usually to represent the wrapped Butterfly (di)graph we use the representation of $\vec{\mathcal{BF}}(d,n)$ by repeating at the end level 0. Hence the reader has to remember that levels 0 and n are identified for $\mathcal{WB\vec{F}}(d,n)$. $\mathcal{WB\vec{F}}(d,n)$ is a d-regular digraph with nd^n vertices; its diameter is $2n-1$. The underlying wrapped Butterfly network will be denoted $\mathcal{WBF}(d,n)$; it is regular of degree $2d$, with diameter $\lfloor \frac{3n}{2} \rfloor$.

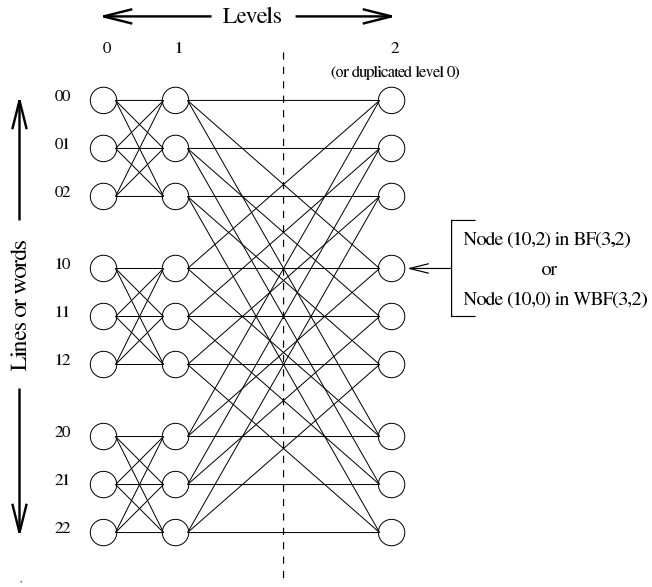

Figure 1: *The graphs $\mathcal{BF}(3,2)$ (multistage version) with 3 levels, or $\mathcal{WBF}(3,2)$ (point-to-point version) by duplicating level 0. For digraphs $\vec{\mathcal{BF}}(3,2)$ or $\mathcal{WB\vec{F}}(3,2)$ the edges must be directed into arcs from left to right .*

1.2 Other definitions and general results

- $\mathcal{K}_d$ will denote the complete graph on d vertices,
- $\mathcal{K}_{d,d}$ will denote the complete bipartite graph where each set of the bipartition has size d,
- G^* will denote the symmetric digraph obtained from the graph G by replacing each edge by two opposite arcs. In particular $\mathcal{K}_d^*$ *(resp.* $\mathcal{K}_{d,d}^*$*)* will denote the complete symmetric *(resp. bipartite)* digraph on d *(resp.* $d \times d$*)* vertices,
- $\mathcal{K}_d^+$ will denote the complete symmetric digraph with a loop on each vertex,
- a circuit or directed cycle of length n will be denoted $\vec{C}_n$, and a dipath of length n $\vec{P}_n$.

- $\vec{\mathcal{K}}_{d,d}$ will denote the directed digraph obtained from $\mathcal{K}_{d,d}$ by orienting each edge from the left part to the right part.

Definition 1.3 *(see [15]) Let G be a directed graph. The* **line digraph** *$L(G)$ of G is the directed graph whose vertices are the arcs of G and whose arcs are defined as follows: there is an arc from a vertex e to a vertex f in $L(G)$ if and only if, in G, the initial vertex of f is the end vertex of e.*

Note that $\mathcal{WB\vec{F}}(d,1)$ is nothing else than $\mathcal{K}_d^+$ and that $\mathcal{B\vec{F}}(d,1)$ is $\vec{\mathcal{K}}_{d,d}$. We will see in section 4 (corollary (**4.1**)) that $\mathcal{WB\vec{F}}(d,2)$ is the line digraph of $\mathcal{K}^*_{d,d}$.

Definition 1.4 *A* **1-difactor** *of a digraph G is a spanning subgraph of G with in and out-degree 1. It corresponds to a partition of the vertices of G into circuits.*

Definition 1.5 *A* **Hamilton cycle (resp. circuit)** *of a graph* (resp. digraph) *is a cycle* (resp. circuit) *which contains every vertex exactly once.*

Definition 1.6 *We will say that a graph* (resp. digraph) *has a* **Hamilton decomposition** *or* **can be decomposed into Hamilton cycles (resp. circuit)** *if its edges* (resp. arcs) *can be partitioned into Hamilton cycles* (resp. circuits).

Remark 1 A Hamilton circuit is a connected 1-difactor.

The existence of one and if possible many edge(arc)-disjoint Hamilton cycles (circuits) in a network can provide advantage for algorithms that make use of a ring structure. Furthermore, the existence of a Hamilton decomposition allows also the message traffic to be evenly distributed across the network. Various results have been obtained on the existence of Hamilton cycles in classical networks (see for example the survey [2, 11]). For example it is well-known that any Cayley graph on an abelian group is Hamiltonian. Furthermore it has been conjectured by Alspach [1] that:

Conjecture 1 **(Alspach)** *Every connected Cayley graph on an abelian group has a Hamilton decomposition.*

This conjecture has been verified for all connected 4-regular graphs on abelian groups in [9]. That includes in particular the toroidal meshes (grids). For the hypercube of dimension $2d$ it is also known that $\mathcal{H}(2d)$ can be decomposed into d Hamilton cycles (see [3, 2]).

Concerning line digraphs it has been shown in [12] that d-regular line digraphs always admit $\lfloor \frac{d}{2} \rfloor$ Hamilton circuits. In the case of de Bruijn or Kautz digraphs which are the simplest line digraphs, partial results have been obtained successively in [6, 14], and near optimal results have been obtained for undirected de Bruijn and Kautz graphs [4].

1.3 Results for the Butterfly networks

The wrapped Butterfly (di)graph is actually a Cayley graph (on a non abelian group) and a line digraph. So the decomposition into Hamilton cycles *(resp. circuits)* of this graph *(resp. digraph)* has received some attention. First it is well-known that $\mathcal{WB\vec{F}}(d,n)$ is Hamiltonian (see [13, page 465] for a proof in the case $d = 2$). In [7], Barth and Raspaud proved that $\mathcal{WBF}(2,n)$ has a Hamilton decomposition answering a conjecture of J. Rowley and D. Sotteau (private communication).

Theorem 1.1 (Barth, Raspaud) *$\mathcal{WBF}(2,n)$ can be decomposed into 2 Hamilton cycles.*

They also gave the following conjecture.

Conjecture 2 (Barth, Raspaud) *For $n \geq 2$, $\mathcal{WBF}(d,n)$ can be decomposed into d Hamilton cycles.*

In his thesis [5] , Barth also stated the following conjecture for the directed case:

Conjecture 3 (Barth) *For $n \geq 2$, $\vec{\mathcal{WBF}}(d,n)$ contains $d-1$ arc-disjoint Hamilton circuits.*

Recall that for $n = 1$ $\vec{\mathcal{WBF}}(d,1)$ is nothing else than $\mathcal{K}_d^+$ which itself is the arc-disjoint sum of $\mathcal{K}_d^*$ and loops. So conjecture (**3**) can be seen as an extension of a theorem of Tillson [17].

Theorem 1.2 (Tillson) *The complete symmetric digraph $\mathcal{K}_d^*$ can be decomposed into $d-1$ Hamilton circuits except for $d = 4$ and 6.*

In this paper we focus mainly on the decomposition of the wrapped Butterfly digraph $\vec{\mathcal{WBF}}(d,n)$. Our main result implies that the number of arc-disjoint Hamilton circuits contained in $\vec{\mathcal{WBF}}(d,n)$ can only increase when n increases.

Proposition 1.1 *If $\vec{\mathcal{WBF}}(d,n)$ contains p arc-disjoint Hamilton circuits, then $\vec{\mathcal{WBF}}(d,n')$ contains also at least p arc-disjoint Hamilton circuits, for any $n' \geq n$.*

This proposition with Tillson's theorem and a special study for $d = 4$ and 6, implies conjecture (**3**).

Theorem 1.3 *For $n \geq 2$, $\vec{\mathcal{WBF}}(d,n)$ contains $d-1$ arc-disjoint Hamilton circuits.*

Furthermore it appears that, except for three cases, for all small values of d, $\vec{\mathcal{WBF}}(d,n)$ can be decomposed into d Hamilton circuits, so we conjecture that:

Conjecture 4 *For $n \geq 2$, $\vec{\mathcal{WBF}}(d,n)$ can be decomposed into d Hamilton circuits, except for ($d = 2$, $n = 2$ or 3) and ($d = 3$, $n = 2$).*

By the proposition (**1.1**) it suffices to prove the conjecture for $n = 2$. Using results of section 4 on conjunction of graphs, we have been able to reduce the study to prime degrees. So conjecture (**4**) would follow from conjecture (**5**).

Conjecture 5 *For any prime number $p > 3$, $\vec{\mathcal{WBF}}(p,2)$ can be decomposed into p Hamilton circuits.*

With a clever computer search, we have been able to prove conjecture (**5**) for any prime less than 12000, leading to the following statement:

Theorem 1.4 *If d is divisible by any number q, $4 \leq q \leq 12000$ then $\vec{\mathcal{WBF}}(d,2)$ and consequently $\vec{\mathcal{WBF}}(d,n)$ has a Hamilton decomposition.*

Finally the methods used in this paper can be applied with other ideas to the undirected case and lead us to prove conjecture (**2**) in a forthcoming paper [8].

Theorem 1.5 *For $n \geq 2$, $\mathcal{WBF}(d,n)$ can be decomposed into d Hamilton cycles.*

2 Circuits and Permutations

2.1 More definitions

First, we will show that the existence of k arc-disjoint Hamilton circuits in $\mathcal{WB}\vec{\mathcal{F}}(d,n)$, is equivalent to the ability to route k *compatible cyclic realizable* permutations between levels 0 and n in $\mathcal{B}\vec{\mathcal{F}}(d,n)$. For this purpose we need some specific definitions.

In the whole paper, π will always denote a permutation of $\mathbb{Z}_d^n$ which associates to x, $\pi(x)$. The **composition $\pi \cdot \pi'$ of two permutations** π and π' is the permutation which associate to the element a the element $\pi(\pi'(a))$.

Definition 2.1 *A permutation π is* **cyclic** *if for some x all the elements $\pi^i(x)$ are distinct for $0 \leq i < d^n$.*

Remark 2 Note that if π is cyclic, then for each x the elements $\pi^i(x)$ are all distinct. In fact to verify that π is cyclic it suffices to verify that for a given x, $\pi^i(x) \neq x$ for $1 \leq i < d^n$. Indeed, if there exists j and k with $j > k$ such that $\pi^j(x) = \pi^k(x)$ then $\pi^{j-k}(x) = x$.

For example, the permutation π which associates to a the element $a+1$ is clearly cyclic as $\pi^i(a) = a + i$.

It follows from the definition of $\mathcal{B}\vec{\mathcal{F}}(d,n)$ that there exists a unique dipath connecting a vertex $(x,0)$ to a vertex (y,n). So we can associate to a permutation π of $\mathbb{Z}_d^n$ a set of dipaths in $\mathcal{B}\vec{\mathcal{F}}(d,n)$ connecting vertex $(x,0)$ to vertex $(\pi(x),n)$ for any x in $\mathbb{Z}_d^n$.

Following the terminology used in multistage interconnection networks, where one wants to connect inputs to outputs via disjoint paths, we introduce the notation of realizable permutation.

Definition 2.2 *A permutation π is* **realizable** *in $\mathcal{B}\vec{\mathcal{F}}(d,n)$ or equivalently $\mathcal{B}\vec{\mathcal{F}}(d,n)$ realizes the permutation π if the d^n associated dipaths from the inputs to the outputs are vertex-disjoint.*

Finally, following the terminology of Eulerian graph theory we say:

Definition 2.3 *A set of k permutations $\pi_0, \pi_1, \cdots, \pi_{k-1}$ realizable in $\mathcal{B}\vec{\mathcal{F}}(d,n)$ is* **compatible** *if the kd^n dipaths from $(x,0)$ to $(\pi_j(x),n)$ for x in $\mathbb{Z}_d^n$ and $0 \leq j \leq k-1$ are arc-disjoint. We will also say that $\mathcal{B}\vec{\mathcal{F}}(d,n)$ realizes k compatible permutations.*

Warning: In the whole paper we are working with permutations which are mathematical objects independent of the graph for which they can be either realizable or compatible. In contrary the realizability or compatibility is a property related to the graphs on which it applies.

2.2 Hamilton circuits and permutations

We are now ready to prove that there is an immediate connection between the existence of compatible cyclic realizable permutations in $\vec{\mathcal{BF}}(d,n)$ and that of arc-disjoint Hamilton circuits in $\mathcal{W}\vec{\mathcal{BF}}(d,n)$.

Lemma 2.1 *$\mathcal{W}\vec{\mathcal{BF}}(d,n)$ contains k arc-disjoint Hamilton circuits if and only if $\vec{\mathcal{BF}}(d,n)$ realizes k compatible cyclic permutations.*

Proof. First let us show how to associate to a cyclic permutation π realizable in $\vec{\mathcal{BF}}(d,n)$ a Hamilton circuit of $\mathcal{W}\vec{\mathcal{BF}}(d,n)$ and conversely.

Let π be a cyclic permutation of $\mathbb{Z}_d^n$. Let x be a given element of $\mathbb{Z}_d^n$ and let P_i be the unique dipath of $\vec{\mathcal{BF}}(d,n)$ joining $(\pi^i(x),0)$ to $(\pi^{i+1}(x),n)$. As π is cyclic all the $\pi^i(x)$ are distinct. So, if π is realizable, the dipaths P_i are vertex-disjoint. Let P_i' be the dipath of $\mathcal{W}\vec{\mathcal{BF}}(d,n)$ obtained from P_i by identifying $(\pi^{i+1}(x),n)$ with $(\pi^{i+1}(x),0)$. Now the end vertex of P_i' is the initial of P_{i+1}' and so, as the $(\pi^i(x),0)$ span the set of vertices of level 0, the concatenation of the dipaths P_i' with $0 \leq i < d^n - 1$ forms a Hamilton circuit of $\mathcal{W}\vec{\mathcal{BF}}(d,n)$.

Conversely, let H be a Hamilton circuit of $\mathcal{W}\vec{\mathcal{BF}}(d,n)$. Let $(x_0,0),\cdots,(x_i,0),\cdots,(x_{d^n-1},0)$ be the vertices we meet successively on level 0 by following the cycle H. Let us consider the permutation defined by $\pi(x_i) = x_{i+1}$. As H is a Hamilton circuit, all the x_i's are distinct so π is cyclic; furthermore all the inside dipaths are vertex-disjoint, so π is a cyclic realizable permutation in $\vec{\mathcal{BF}}(d,n)$.

To prove the lemma it suffices to note that the definition of compatible permutations has been done in order that the dipaths associated to the permutation are arc-disjoint and so their concatenation form arc-disjoint Hamilton circuits, and conversely (see Figure (**2**)). □

3 Recursive construction

3.1 Recursive decomposition of $\vec{\mathcal{BF}}(d,n)$

The permutation network $\vec{\mathcal{BF}}(d,n)$ has a simple recursive property: the $n+1$ first levels of $\vec{\mathcal{BF}}(d,n+1)$ form d vertex-disjoint subgraphs isomorphic to $\vec{\mathcal{BF}}(d,n)$. We shall call them left Butterflies. If the elements of $\mathbb{Z}_d^{n+1}$ are denoted $y = (ax) \in \mathbb{Z}_d \times \mathbb{Z}_d^n$, then each left Butterfly connects the set of vertices having the same left part a. So we will label a left Butterfly by $\mathcal{B}_{left}(a)$. In the same way, the two last levels of $\vec{\mathcal{BF}}(d,n+1)$ are built with d^n disjoint subgraphs isomorphic to $\vec{\mathcal{BF}}(d,1) = \vec{\mathcal{K}}_{d,d}$, that we shall call right Butterflies; each right Butterfly connects all the vertices having the same right part x and we will label it by $\vec{\mathcal{K}}_{d,d}(x)$.

We can summarize the situation as follows:

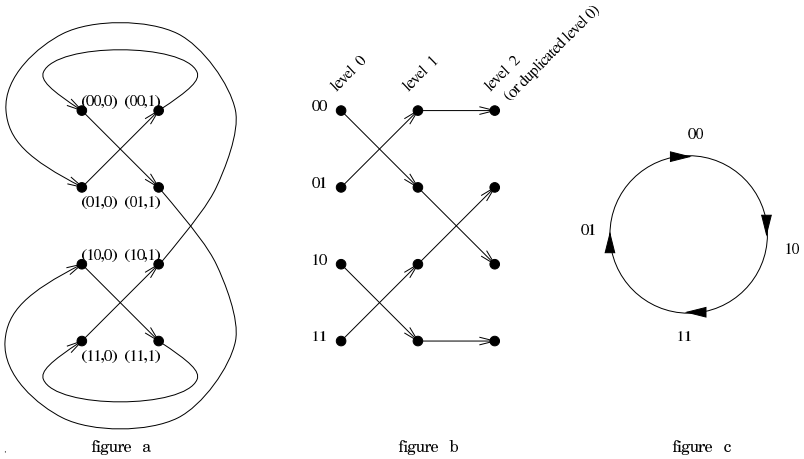

Figure 2: *A Hamilton circuit of $\mathcal{WB\vec{F}}(2,2)$ (figure a) or equivalently the associated permutation realizable in $\mathcal{B\vec{F}}(2,2)$ (figure b) and the cyclic permutation which is used (figure c).*

- vertices of $\mathcal{B\vec{F}}(d, n+1)$ are denoted (ax, l),
- the left Butterfly labeled by $a \in \mathbb{Z}_d$ is formed by the vertices $a*$ of the $n+1$ first levels. It is denoted $\mathcal{B}_{left}(a)$,
- the right Butterfly with label $x \in \mathbb{Z}_d^n$ is formed by the vertices $*x$ of the 2 last levels. It is denoted $\vec{\mathcal{K}}_{d,d}(x)$.

Remark 3 In $\mathcal{B\vec{F}}(d, n+1)$, vertices of level $n+1$ are shared by the left and right Butterflies, the outputs of the left Butterflies being considered as the inputs of the right Butterflies. Moreover all the subgraphs defined above are arc-disjoint.

Figure (**3**) displays such a recursive decomposition.

3.2 Iterative Construction

We will now give a simple construction which enables us to construct p compatible cyclic realizable permutations in $\mathcal{B\vec{F}}(d, n+1)$ from p compatible cyclic realizable permutations in $\mathcal{B\vec{F}}(d, n)$.

In what follows we will use the letter M to indicate a permutation of $\mathbb{Z}_d$ and M_x to denote a permutation realizable in the right Butterfly $\vec{\mathcal{K}}_{d,d}(x)$. The letter M is chosen as the initial of "matching"; indeed if M_x is a permutation of $\mathbb{Z}_d$ realizable in $\vec{\mathcal{K}}_{d,d}(x)$ then the arcs joining ax to $M_x(a)x$ form a perfect matching in $\vec{\mathcal{K}}_{d,d}(x)$ as they are disjoint.

To be able to prove an inductive lemma we need another definition.

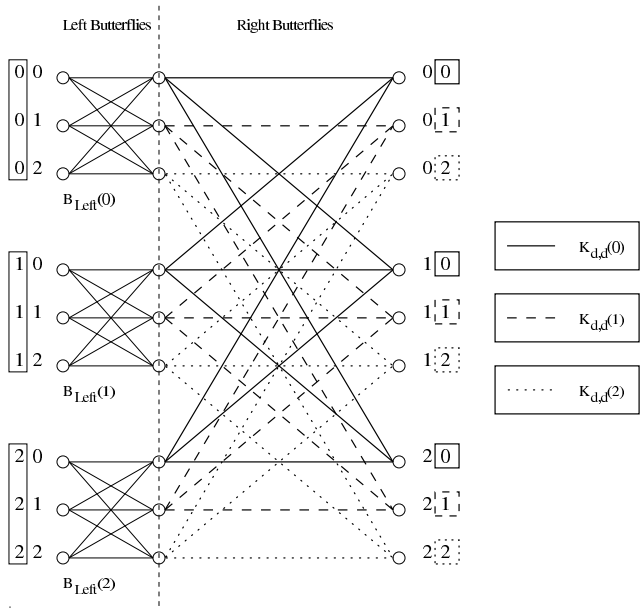

Figure 3: *The recursive decomposition of* $\mathcal{BF}(3,2)$. *To obtain the directed version* $\vec{\mathcal{BF}}(3,2)$ *the edges must be directed into arcs from left to right. The vertices are denoted* $y = (ax) \in \mathbb{Z}_3 \times \mathbb{Z}_3^1$. *In* $\vec{\mathcal{BF}}(3,2)$ *the 2 first levels form 3 vertex-disjoint subgraphs, each one isomorphic to* $\vec{\mathcal{BF}}(3,2-1)$. *These 3 subgraphs are labeled* $\mathcal{B}_{left}(a)$. *In the same way, the 2 last levels of* $\vec{\mathcal{BF}}(3,2)$ *are built with* 3^1 *disjoint subgraphs isomorphic to* $\vec{\mathcal{BF}}(3,1) = \vec{\mathcal{K}}_{d,d}$ *labeled* $\vec{\mathcal{K}}_{d,d}(x)$.

Definition 3.1 *A* **family (or multiset) of permutations** *satisfies the* **cyclic property** *if the composition of the permutations of the family is a cyclic permutation for any order of the composition.*

We use in purpose the word "family" as there might be identical permutation inside. That is the case in the following useful example where all the permutations are identical except one.

Example 1 Let the family $\mathcal{M}_j$ consist of the d^n permutations of $\mathbb{Z}_d$: $M_{x,j}$, where $x \in \mathbb{Z}_d^n$, defined by $M_{x,j}(a) = a+j$ for $x \neq 0$ and $M_{x,j}(a) = a+j+1$ for $x = 0$. Then the family $\mathcal{M}_j$ satisfies the cyclic property. Indeed, consider the permutation obtained by the composition of these d^n permutations in any order; this permutation associates to the element a of $\mathbb{Z}_d$ the element $a + (d^n - 1)j + j + 1 = a + d^n j + 1 = a + 1$ and so is clearly a cyclic permutation of $\mathbb{Z}_d$.

Lemma 3.1 **(Inductive lemma)** *Let* π *be a cyclic permutation realizable in* $\vec{\mathcal{BF}}(d,n)$ *and let* $\mathcal{M} = (M_x,\ x \in \mathbb{Z}_d^n)$ *be a family of* d^n *permutations satisfying the cyclic property and such that* M_x *is realizable in* $\vec{\mathcal{K}}_{d,d}(x)$. *Then the permutation* $f_{(\pi,\mathcal{M})}$ *of* $\mathbb{Z}_d^{n+1}$ *defined by* $f_{(\pi,\mathcal{M})}(ax) = b\pi(x)$ *where* $b = M_{\pi(x)}(a)$, *is a cyclic permutation realizable in* $\vec{\mathcal{BF}}(d,n+1)$.

Proof. First let us show that $f_{(\pi,\mathcal{M})}$ is a cyclic permutation. To show that $f_{(\pi,\mathcal{M})}$ is cyclic, it suffices, by remark (**2**), to show that $f^i_{(\pi,\mathcal{M})}(ax) \neq ax$ for $1 \leq i \leq d^{n+1} - 1$. Suppose that $f^i_{(\pi,\mathcal{M})}(ax) = ax$ for some i. By definition $f^i_{(\pi,\mathcal{M})}(ax) = a'\pi^i(x)$. So $\pi^i(x) = x$, which implies that $i = kd^n$. But for $i = d^n$, a' is the image of a by the composition of the d^n elements of $\mathcal{M}$ in some order; so as $\mathcal{M}$ has the cyclic property, $a' = \sigma(a)$, where σ is a cyclic permutation. Therefore, $f^{kd^n}_{(\pi,\mathcal{M})}(ax) = \sigma^k(a)x \neq ax$ for $1 \leq k < d$. So for any i, $1 \leq i \leq d^{n+1} - 1$, $f^i_{(\pi,\mathcal{M})}(ax) \neq ax$.

Then it remains to show that $f_{(\pi,\mathcal{M})}$ is realizable in $\vec{\mathcal{BF}}(d, n+1)$. The dipath associated to $f_{(\pi,\mathcal{M})}$ from $(ax, 0)$ to $(b\pi(x), n+1)$ consists of the dipath from $(ax, 0)$ to $(a\pi(x), n)$ in $\mathcal{B}_{left}(a)$ associated to the permutation π of $\mathcal{B}_{left}(a)$ (which is isomorphic to $\vec{\mathcal{BF}}(d, n)$) and then of the arc joining $(a\pi(x), n)$ to $(b\pi(x), n+1)$ in $\vec{\mathcal{K}}_{d,d}(\pi(x))$ defined by the matching associated to the permutation $M_{\pi(x)}$, that is $b = M_{\pi(x)}(a)$. We claim that the dipaths joining two distinct inputs $(ax, 0)$ and $(a'x', 0)$ to their outputs are vertex-disjoint and so $f_{(\pi,\mathcal{M})}$ is realizable. Indeed, if $a \neq a'$ their first parts are in two different $\mathcal{B}_{left}(a)$ and $\mathcal{B}_{left}(a')$ and the last arcs are disjoint as either $x \neq x'$ or $x = x'$ and $M_{\pi(x)}$ is realizable in $\vec{\mathcal{K}}_{d,d}(\pi(x))$. If $a = a'$, π being realizable the first dipaths are vertex-disjoint and as $x \neq x'$ the last arcs belong to two different $\vec{\mathcal{K}}_{d,d}$. □

Corollary 3.1 *If there exist p compatible cyclic realizable permutations in $\vec{\mathcal{BF}}(d, n)$, then there exist p compatible cyclic realizable permutations in $\vec{\mathcal{BF}}(d, n+1)$.*

Proof. For $0 \leq j \leq p-1$ let $\mathcal{M}_j$ be the family of d^n permutations $M_{x,j}$ defined in example (**1**), that is $M_{x,j}(a) = a + j$ for $x \neq 0$ and $M_{x,j}(a) = a + j + 1$ for $x = 0$. Note that the permutation $M_{x,j}$ is realizable in $\vec{\mathcal{K}}_{d,d}(x)$. Let $\pi_0, \ldots, \pi_j, \ldots, \pi_{p-1}$, be p compatible cyclic realizable permutations of $\vec{\mathcal{BF}}(d, n)$. By lemma (**3.1**) for each j the $f_{(\pi_j,\mathcal{M}_j)}$ are cyclic realizable permutations of $\vec{\mathcal{BF}}(d, n+1)$. It remains to show that these permutations are compatible. First the associated dipaths are arc disjoint in the left Butterflies $\mathcal{B}_{left}(a)$, the π_j are compatible; secondly for a given x the permutations $M_{x,j}$ with $0 \leq j \leq p-1$ are themselves compatibles (i.e. the associated matchings are arc-disjoint). Indeed, for $x \neq 0$ the arcs $(a, a+j)$ and $(a, a+j')$ are arc-disjoint (as $j \neq j'$ and $0 \leq j \leq p-1 \leq d-1$ and $0 \leq j' \leq p-1 \leq d-1$; similarly, for $x = 0$ the arcs $(a, a+j+1)$ and $(a, a+j'+1)$ are arc-disjoint. □

Now, we are ready to prove our main proposition stated in the introduction.

Proposition 3.1 **(Main)** *If $W\vec{\mathcal{BF}}(d, n)$ contains p arc-disjoint Hamilton circuits, then $W\vec{\mathcal{BF}}(d, n')$ contains also at least p arc-disjoint Hamilton circuits, for any $n' \geq n$.*

Proof. The result for $n' = n + 1$ follows from corollary (**3.1**) and lemma (**2.1**). A recursive application of this property gives the above proposition. □

For an example of the construction see Figure (**4**).

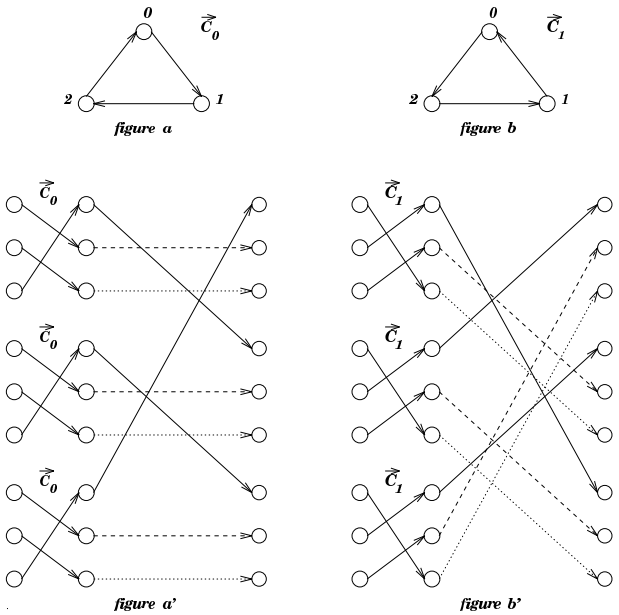

Figure 4: *Two Hamilton circuits (figures a′ and b′) of $\vec{\mathcal{BF}}(3,2)$ are obtained from two Hamilton circuits of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(3,1) = \mathcal{K}_3^+$ by the construction of lemma (**3.1**). Figures (a) and (b) show two arc-disjoint Hamilton circuits of $\mathcal{K}_3^+$, $(\vec{C}_0 \mid x \to x+1 \pmod 3)$ and $(\vec{C}_1 \mid x \to x+2 \pmod 3)$. We used the families $\mathcal{M}_0$ (figure a′) and $\mathcal{M}_1$ (figure b′) defined in the proof of lemma (**??**).*

3.3 Consequences

Corollary 3.2 *$\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2,n)$ can be decomposed into two Hamilton circuits as soon as $n \geq 4$. For $1 \leq n \leq 3$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2,n)$ admits only one Hamilton circuit.*

Proof. A computer search has given a decomposition of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2,4)$ into two arc-disjoint Hamilton circuits. Therefore by proposition (**3.1**) $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2,n)$ has a Hamilton decomposition, for any $n \geq 4$. For $1 \leq n \leq 3$, an exhaustive computer search shows that there cannot exist two arc-disjoint Hamilton circuits. □

Corollary 3.3 *$\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(3,n)$ can be decomposed into three Hamilton circuits as soon as $n \geq 3$. For $1 \leq n \leq 2$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(3,n)$ admits only two arc-disjoint Hamilton circuits.*

Proof. That follows from the existence of a Hamilton decomposition of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(3,3)$ obtained by computer (figures of decompositions available on demand). □

Now we are able to prove Barth's conjecture (**3**).

Theorem 3.2 *For $n \geq 2$, $\mathcal{WBF}(d,n)$ contains $d-1$ arc-disjoint Hamilton circuits.*

Proof. By Tillson's decomposition ((**1.2**)), for $d \neq 4$, and $d \neq 6$, $\mathcal{WBF}(d,1) = \mathcal{K}_d^+$ contains $d-1$ arc-disjoint Hamilton circuits. So by proposition (**3.1**), for $d \neq 4$ and $d \neq 6$, $\mathcal{WBF}(d,n)$ contains at least $d-1$ arc-disjoint Hamilton circuits. For $d = 4$ *(resp. 6)*, we have found by computer search 4 *(resp. 6)* arc-disjoint Hamilton circuits in $\mathcal{WBF}(4,2)$ *(resp.* $\mathcal{WBF}(6,2)$*)*. So by proposition (**3.1**), $\mathcal{WBF}(4,n)$ *(resp.* $\mathcal{WBF}(6,n)$*)* contains 4 *(resp. 6)* arc-disjoint Hamilton circuits. □

As seen in the proof above for $d = 4, 6$ there exists for $n \geq 2$ a Hamilton decomposition of $\mathcal{WBF}(d,n)$. These results and those of the next section lead us to propose the following conjecture, which would completely close the study of the Hamilton decomposition of $\mathcal{WBF}(d,n)$.

Conjecture 6 *For $d \geq 4$ and $n \geq 2$, $\mathcal{WBF}(d,n)$ can be decomposed into Hamilton circuits.*

By proposition (**3.1**) it suffices to prove the conjecture for $n = 2$ or equivalently, as $\mathcal{WBF}(d,2) = L(\mathcal{K}^*_{d,d})$ (see corollary (**4.1**)) that $\mathcal{K}^*_{d,d}$ admits d compatible Eulerian tours (see [12]).

4 Decomposition of $\mathcal{WBF}(d,2)$ into Hamilton circuits

4.1 Line digraphs and conjunction

We need some more definitions and results concerning *conjunction*, *line digraphs* and *de Bruijn digraphs*.

Definition 4.1 *(see [2])*

1. *The* **conjunction** *$G_1 \cdot G_2$ of two digraphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the digraph with vertex-set $V_1 \times V_2$ and an arc joining (u_1, u_2) to (v_1, v_2) if and only if there is an arc joining u_1 to v_1 in G_1 and an arc joining u_2 to v_2 in G_2.*
2. *If A and B are two digraphs defined on the same set of vertices with no arc in common, we denoted by $A \oplus B$ the* **arc-disjoint union (sum)** *of them, that is the digraph on the same set of vertices having as arcs the union of those of A and B.*
3. *cG will denote the digraph made of c disjoint copies of G.*
4. *$L^k(G)$ will denote the k iterated line digraph of G, that is $L^k(G) = L(L^{k-1}(G))$.*

For example $\mathcal{K}^*_{d,d} = \mathcal{K}_d^+ \cdot \vec{C}_2$ and $\mathcal{WBF}(2,4) = A \oplus B$ where A and B are the two arc-disjoint Hamilton circuits of $\mathcal{WBF}(2,4)$.

Properties 4.1

$$F \cdot G = G \cdot F$$

$$L(F \cdot G) = L(F) \cdot L(G)$$

$$(F \cdot G) \cdot H = F \cdot (G \cdot H) = F \cdot G \cdot H$$

$$(A \oplus B) \oplus C = A \oplus (B \oplus C) = A \oplus B \oplus C$$

$$(A \oplus B) \cdot F = (A \cdot F) \oplus (B \cdot F)$$

Proof. These results are clear from the definitions. □

There is a very strong connection between the *de Bruijn* digraph and the wrapped Butterfly digraph. We recall the definition of the de Bruijn digraph:

Definition 4.2 *The* **de Bruijn digraph** $\vec{\mathcal{B}}(d,n)$ *of out-degree* d *and diameter* n *has as vertices the words of length* n *on an alphabet of* d *letters. Vertex* $x_0 \dots x_{n-1}$ *is joined by an arc to the vertices* $x_1 \dots x_{n-1}\alpha$ *where* α *is any letter from the alphabet.*

Proposition 4.2

$$\vec{\mathcal{B}}(d,n) = L^{n-1}(\mathcal{K}_d^+) \tag{1}$$

$$\vec{\mathcal{B}}(d_1 d_2, n) = \vec{\mathcal{B}}(d_1,n) \cdot \vec{\mathcal{B}}(d_2,n) \tag{2}$$

$$\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n) = \vec{\mathcal{B}}(d,n) \cdot \vec{C}_n = L^{n-1}(\mathcal{K}_d^+ \cdot \vec{C}_n) \tag{3}$$

$$\mathcal{B}\vec{\mathcal{F}}(d,n) = \vec{\mathcal{B}}(d,n) \cdot \vec{P}_n \tag{4}$$

$$\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1 d_2, n) = \mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1,n) \cdot \vec{\mathcal{B}}(d_2,n) \tag{5}$$

Proof. Equality (**1**) is well known, and even sometimes considered as the proper definition of de Bruijn digraphs (see [10, 15]).

Result (**2**) can be found in [16] and can be proved as follows: $\vec{\mathcal{B}}(d_1 d_2, n) = L^{n-1}(\mathcal{K}^+_{d_1 d_2})$ from (**1**), but $\mathcal{K}^+_{d_1 d_2} = \mathcal{K}^+_{d_1} \cdot \mathcal{K}^+_{d_2}$. By properties (**4.1**), $L^{n-1}(\mathcal{K}^+_{d_1} \cdot \mathcal{K}^+_{d_2}) = L^{n-1}(\mathcal{K}^+_{d_1}) \cdot L^{n-1}(\mathcal{K}^+_{d_2})$ which is indeed $\vec{\mathcal{B}}(d_1,n) \cdot \vec{\mathcal{B}}(d_2,n)$.

Result (**3**) is implicit in different papers. It can be obtained by considering the following isomorphism from $\vec{\mathcal{B}}(d,n)\cdot\vec{C}_n$ to $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$. To the vertex (x,l) in $\vec{\mathcal{B}}(d,n)\cdot\vec{C}_n$ with $x=x_0x_1\cdots x_{n-1}$, and $l\in\mathbb{Z}_n$, we associate the vertex $\phi((x,l))=(x',l)$ in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$, where $x'=x'_{n-1}x'_{n-2}\cdots x'_0$ and $x'_i=x_{i-l}$. By definitions ((**4.1**)-**1**) and (**4.2**), the out-neighbors of (x,l) in $\vec{\mathcal{B}}(d,n)\cdot\vec{C}_n$ are the vertices $(y,l+1)$ with $y=y_0y_1\cdots y_{n-1}$ such that $y_i=x_{i+1}$ for $i\neq n-1$, and $y_{n-1}=\alpha$, α being any letter from the alphabet. The associated vertices in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$ are $\phi((y,l+1))=(y',l+1)$ where $y'=y'_{n-1}y'_{n-2}\cdots y'_0$ and $y'_i=y_{i-l-1}$. For $i-l-1\neq n-1$, or equivalently $i\neq l$, $y'_i=x_{i-l}=x'_i$, and for $i=l$, $y'_i=\alpha$. So by definition (**1.2**), the vertices $(y',l+1)$ are exactly the out-neighbors of (x',l) in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$. The second part of the equality is due to the fact that $L^{n-1}(\vec{C}_n)=\vec{C}_n$, hence $L^{n-1}(\mathcal{K}_d^+)\cdot\vec{C}_n=L^{n-1}(\mathcal{K}_d^+)\cdot L^{n-1}(\vec{C}_n)=L^{n-1}(\mathcal{K}_d^+\cdot\vec{C}_n)$.

An example is displayed in Figure (**5**). Result (**4**) can be proved in the same way as (**3**).

The last equality follows directly from (**2**) and (**3**). □

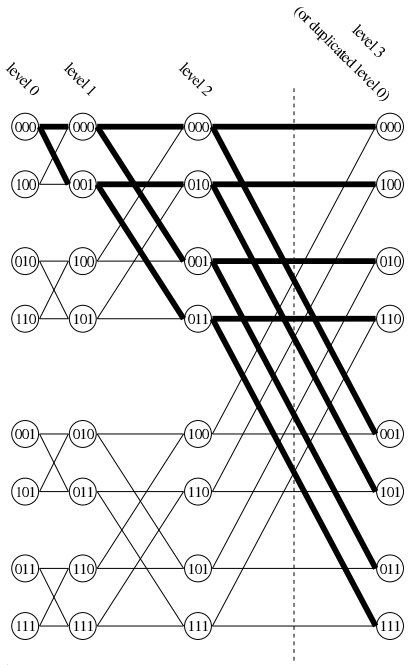

Figure 5: *The graph* $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2,3)$ *as a conjunction of* $\vec{\mathcal{B}}(2,3)$ *with* $\vec{C}_3$.

Corollary 4.1 $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,2)=L(\mathcal{K}^*_{d,d})$.

Proof. Follows from proposition (**4.2**) equality (**3**) for $n = 2$. □

Lemma 4.1 *When r and s are relatively prime, $\vec{C}_{qs} \cdot \vec{C}_{qr} = q\vec{C}_{qsr}$.*

Proof. $\vec{C}_{qs} \cdot \vec{C}_{qr}$ is a regular digraph with in and out-degree 1. So it is the union of circuits. Starting from a vertex (u, v) we find at distance i the vertex $(u + i, v + i)$ where $u + i$ *(resp.* $v + i$*)* has to be taken modulo qs *(resp.* qr*)*. So the length of any circuit is the smallest common multiple of qs and qr, that is qrs as r and s are relatively prime. As the number of vertices in the digraph is q^2rs there are q such cycles. □

Proposition 4.3 $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1, n) \cdot \mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2, n) = n\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2, n)$

Proof. Let $G = \mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1, n) \cdot \mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2, n)$. By property (**3**) of proposition (**4.2**), we have $G = (\vec{\mathcal{B}}(d_1, n) \cdot \vec{C}_n) \cdot (\vec{\mathcal{B}}(d_2, n) \cdot \vec{C}_n)$. As $\vec{C}_n \cdot \vec{C}_n = n\vec{C}_n$ (from lemma (**4.1**) with $q = n$ and $s = r = 1$), then we obtain:

$$G = \vec{\mathcal{B}}(d_1, n) \cdot \vec{\mathcal{B}}(d_2, n) \cdot (n\vec{C}_n) = n(\vec{\mathcal{B}}(d_1, n) \cdot \vec{\mathcal{B}}(d_2, n) \cdot \vec{C}_n) = n\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2, n).$$

□

Corollary 4.2 *If d_1 and d_2 are relatively prime, and if $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1, n)$* (resp. $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2, n)$*) admits a_1* (resp. a_2*) arc-disjoint Hamilton circuits, then $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2, n)$ admits a_1a_2 arc-disjoint Hamilton circuits.*

Proof. Let $\vec{C}_{nd_1^n}$ *(resp.* $\vec{C}_{nd_2^n}$*)* be a Hamilton circuit in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1, n)$ *(resp.* $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2, n)$*)*. From lemma (**4.1**), the conjunction $\vec{C}_{nd_1^n} \cdot \vec{C}_{nd_2^n}$ is a set of n circuits of length $nd_1^nd_2^n$.

As $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2, n)$ has $nd_1^nd_2^n$ vertices, the 1-difactor $\vec{C}_{nd_1^n} \cdot \vec{C}_{nd_2^n}$ consists of n circuits each one being a Hamilton circuit of a connected component of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1, n) \cdot \mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2, n)$ isomorphic to $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2, n)$. So, the conjunction of one Hamilton circuit of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1, n)$ with one Hamilton circuit of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_2, n)$ provides one Hamilton circuit in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2, n)$. Applying this results to the a_1a_2 different ordered pairs of circuits, provides a_1a_2 arc-disjoint Hamilton circuits in $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d_1d_2, n)$. □

So by corollary (**4.2**) it is enough to prove conjecture (**6**) for every power p^i of a prime number p.

4.2 Reduction to the case where p is prime

We would like to prove that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d, 2) = \vec{\mathcal{B}}(d, 2) \cdot \vec{C}_2$ has a Hamilton decomposition. That appears quite difficult. However, we will prove that for $n \geq 3$, $\vec{\mathcal{B}}(d, 2) \cdot \vec{C}_n$ has a Hamilton decomposition. Such a decomposition will then be sufficient to reduce the problem to the case of prime degrees.

Lemma 4.2 *For any number $n \geq 3$ and any prime p, $\vec{\mathcal{B}}(p,2)\cdot\vec{C}_n$ can be decomposed into p Hamilton circuits.*

Proof. Let the nodes of $\vec{\mathcal{B}}(p,2) \cdot \vec{C}_n$ be labeled (xy,l) with $x \in \mathbb{Z}_d$, $y \in \mathbb{Z}_d$ and $l \in \mathbb{Z}_n$. The digraph $\vec{\mathcal{B}}(p,2) \cdot \vec{C}_n$ is similar to the wrapped butterfly digraph, so we can also define a multistage network obtained by duplicating the level 0 into a level n. Formally this multistage network is $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_n$ where $\vec{P}_n$ is a directed path of length n (.i.e. with $n+1$ vertices); its vertices will be labeled (xy,l) with $x \in \mathbb{Z}_d$, $y \in \mathbb{Z}_d$ and $l \in \{0,1,\cdots,n\}$.

Like in section 2, we can define a notion of realizable permutation in $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_n$ except that now there is more than one dipath connecting $(xy,0)$ to $(\pi(xy),n)$. We will say that $\vec{\mathcal{B}}(p,2)\cdot\vec{P}_n$ realizes k compatible permutations of $\mathbb{Z}_p^2$, $\pi_0,\pi_1,\ldots,\pi_{k-1}$ if there exist kp^2 dipaths $P_j(xy)$, $0 \leq j \leq k-1$, $xy \in \mathbb{Z}_p^2$, where $P_j(xy)$ connects $(xy,0)$ to $(\pi_j(xy),n)$ in $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_n$ satisfying the following properties. For a given j the p^2 dipaths $P_j(xy)$ are vertex-disjoint (realizability property) and all the kp^2 dipaths $P_j(xy)$ are arc-disjoint (compatibility property).

Using the same argument than in lemma (**2.1**), we can state that $\vec{\mathcal{B}}(p,2) \cdot \vec{C}_n$ can be decomposed into p Hamilton circuits if and only if $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_n$ realizes p compatible cyclic permutations.

We will show by induction that $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_n$ realizes p compatible cyclic permutations; more exactly we will prove that if the property is true for n, it is also true for $n+3$. First we give for $n = 3, 4$ and 5 the dipaths $P_j(xy)$ associated to compatible cyclic permutations.

In all the dipaths that we consider, a vertex (xy,l) is followed by a vertex $(yx',l+1)$ with $x' = g_l(x,y,j) = ax + f(y) + cj$, where a, f and c depend on the level l.

- For any j, the dipaths $P_j(xy)$ are vertex-disjoint if and only if at each level two distinct vertices (x_1y_1,l) and (x_2y_2,l) are followed by two distinct vertices $(y_1x_1',l+1)$ and $(y_2x_2',l+1)$. As p is a prime, that is realized if and only if the coefficient a of x in $g_l(x,y,j)$ is different to 0. Indeed, suppose $y_2x_2' = y_1x_1'$ then $y_2 = y_1$ and $x_2' = x_1'$. So $ax_2 + f(y_2) + cj = ax_1 + f(y_1) + cj$ and as $y_2 = y_1$, that implies $ax_2 = ax_1$, which in turn implies, as p is a prime number, either $a = 0$ or $x_2 = x_1$.

- Similarly the dipaths $P_j(xy)$ are arc-disjoint if and only if for given l, x, y, $g_l(x,y,j) = g_l(x,y',j)$ are different. That is satisfied if and only if $c \neq 0$, as p is a prime number.

In order to simplify the notation we omit in the labels of the vertices the values of the levels; as a vertex of level l is always followed by a vertex of level $l+1$.

4.2.1 Initial constructions

Let δ_0 denote the function of $\mathbb{Z}_p$ into $\{0,1\}$:

$$\delta_0(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0 \end{cases}$$

$n = 3$

$$P_j(xy) = \quad xy \quad y(x+y+j) \quad (x+y+j)(x+1) \quad (x+1)(y+\delta_0(x+1))$$

$n = 4$

$$P_j(xy) = \quad xy \quad y(x+j) \quad (x+j)(y+j) \quad (y+j)(x+1) \quad (x+1)(y+\delta_0(x+1))$$

Figure (**6**) shows one decomposition of $\vec{\mathcal{B}}(3,2) \cdot \vec{C}_4$ into circuits. To produce a clearer figure, vertices ab on odd levels are ranked lexicographically and those on even levels in the following order: $ab < a'b'$ if $b < b'$ or $b = b'$ and $a < a'$.

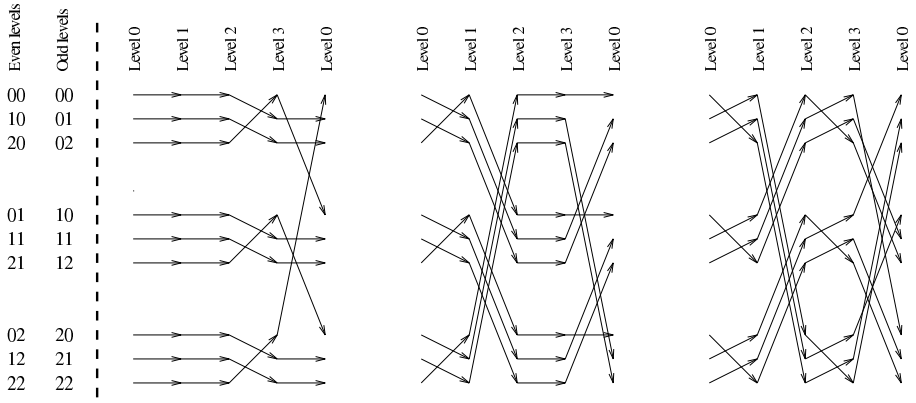

Figure 6: *A decomposition of* $\vec{\mathcal{B}}(3,2) \cdot \vec{C}_4$*, presented with a special ranking of the vertices.*

$n = 5$ **and** $p \neq 2$

$$P_j(xy) = \quad xy \quad y(x+y+j) \quad (x+y+j)(x+2j) \quad (x+2j)y \quad y(x+1) \quad (x+1)(y+j+\delta_0(x+1))$$

$n = 5$ **and** $p = 2$

$$P_j(xy) = \quad xy \quad y(x+y+j+1) \quad (x+y+j+1)(y+j) \quad (y+j)(x+j+1) \quad (x+j+1)y \quad y(x+1)$$

In all the cases one can easily verify that the functions $g_l(x, y, j)$ are of the form $ax + f(y) + cj$ with $a \neq 0$ and $c \neq 0$. For example, in the construction for $n = 3$, the functions implicitly defined are:

$$\begin{array}{ccc} (X,Y) & \overset{X'=aX+f(Y)+cj}{\rightarrow} & (Y,X') \\ (x,y) & \overset{X'=X+Y+j}{\rightarrow} & (y,x+y+j) \\ (y,x+y+j) & \overset{X'=Y-X-j+1}{\rightarrow} & (x+y+j,x+1) \\ (x+y+j,x+1) & \overset{X'=X-Y-j+1+\delta_0(Y)}{\rightarrow} & (x+1,y+\delta_0(x+1)) \end{array}$$

To complete the proof it remains to note that in the three first cases the permutation induced by the construction $\pi(xy) = (x+1)(y+cj+\delta_0(x+1))$ is cyclic, and that in the case $n = 5$, $p = 2$ $\pi(xy) = y(x+1)$ is also cyclic as $p = 2$.

4.2.2 Induction step

The induction step follows from two facts. First, it can be easily seen that $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_{n+m}$ realizes p compatible permutations π_j, $0 \leq j \leq p-1$, if and only if there exist two sets of permutations π'_j and π''_j, $0 \leq j \leq p-1$, such that:

- for $0 \leq j \leq p-1$, $\pi_j = \pi'_j \pi''_j$,
- $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_n$ realizes the p compatible permutations π'_j, $0 \leq j \leq p-1$,
- $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_m$ realizes the p compatible permutations π''_j, $0 \leq j \leq p-1$.

Secondly, $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_3$ realizes p compatible permutations π_j, $0 \leq j \leq p-1$, such that each $\pi_j = e$ is the identity permutation. Indeed, let us consider the dipaths:

$$P_j(xy) = \quad xy \quad y(x+y+j) \quad (x+y+j)x \quad xy$$

Once again a vertex XY of level l is joined to a vertex YX' of level $l+1$ with $X' = g_l(X,Y,j) = aX + f(Y) + cj$ with $a \neq 0$ and $c \neq 0$.

So if $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_n$ realizes p compatible permutations π'_j then $\vec{\mathcal{B}}(p,2) \cdot \vec{P}_{n+3}$ realizes the same compatible permutations.

So we can conclude by induction that $\vec{\mathcal{B}}(p,2) \cdot \vec{C}_n$ can be decomposed into p Hamilton circuits for any number $n \geq 3$. □

Theorem 4.3 *If a digraph G with at least 3 vertices, contains k arc-disjoint Hamilton circuits, then $\vec{\mathcal{B}}(d,2) \cdot G$ contains dk arc-disjoint Hamilton circuits.*

Proof. First we prove the result for d prime. By hypothesis $G \supset \bigoplus_{0\leq i<k-1} \vec{C}_l^i$, where l being the number of vertices of G is greater than or equal to 3. Hence

$$\vec{\mathcal{B}}(d,2)\cdot G \supset \vec{\mathcal{B}}(d,2)\cdot \bigoplus_{0\leq i<k-1} \vec{C}_l^i = \bigoplus_{0\leq i<k-1} \vec{\mathcal{B}}(d,2)\cdot \vec{C}_l^i$$

From lemma (**4.2**) $\vec{\mathcal{B}}(d,2)\cdot \vec{C}_l = \bigoplus_{0\leq j\leq d-1} \vec{C}^j_{d^2l}$. So, $\vec{\mathcal{B}}(d,2)\cdot G \supset \bigoplus_{0\leq i<k-1} \bigoplus_{0\leq j\leq d-1} \vec{C}^{i,j}_{d^2l}$ which gives $\vec{\mathcal{B}}(d,2)\cdot G \supset \bigoplus_{0\leq m\leq kd-1} \vec{C}^m_{d^2l}$.

Suppose now that the result holds for all integers strictly less than d. If d is prime we just proved the result. Otherwise $d = d_1p$ where p is a prime and $d_1 < d$. By proposition **(4.2)-2**, $\vec{\mathcal{B}}(d,2) = \vec{\mathcal{B}}(p,2)\cdot\vec{\mathcal{B}}(d_1,2)$. As a consequence $\vec{\mathcal{B}}(d,2)\cdot G = \vec{\mathcal{B}}(p,2)\cdot(\vec{\mathcal{B}}(d_1,2)\cdot G)$. By induction $G' = \vec{\mathcal{B}}(d_1,2)\cdot G$ contains at least d_1k arc-disjoint Hamilton circuits. Moreover p being prime $G = \vec{\mathcal{B}}(p,2)\cdot G'$ will contain $pd_1k = dk$ arc-disjoint Hamilton circuits. □

When G can be decomposed into Hamilton circuits the above theorem can be restated as:

Theorem 4.4 *If G with more than 3 vertices can be decomposed into Hamilton circuits, then $\vec{\mathcal{B}}(d,2)\cdot G$ can also be decomposed into Hamilton circuits.*

Corollary 4.3 *If $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,2)$ with $d \neq 1$ can be decomposed into Hamilton circuits, then $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(qd,2)$ can also be decomposed into Hamilton circuits for any integer q.*

Proof. Just apply theorem (**4.4**) to $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(qd,2)$ which is by proposition (**4.2**) $\vec{\mathcal{B}}(q,2)\cdot\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,2)$. Note that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(1,2)$ has only 2 vertices so the corollary cannot be applied for $d = 1$. □

Example 2 As $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(4,2)$ has a Hamilton decomposition then $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(4q,2)$ has a Hamilton decomposition for any integer q. In particular $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2^i,2)$ has a Hamilton decomposition for $i \geq 2$.

Corollary 4.4 *To prove conjecture (**6**) it suffices to prove that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(p,2)$ has a Hamilton decomposition for any prime $p \geq 5$.*

Proof. Let d be a non prime number. If d has a prime factor p different from 2 or 3, by corollary (**4.3**), it suffices to prove the conjecture for $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(p,2)$. If $d \geq 4$ has only prime factors equal to 2 or 3, then $d = 2^i3^j$ with $i + j \geq 2$. A computer search shows that $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(4,2)$, $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(6,2)$ and $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(9,2)$ have a Hamilton decomposition. So, according to corollary (**4.3**), $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(2^i3^j,2)$ with $i+j \geq 2$ has a Hamilton decomposition. □

Remark 4 Although it is not the purpose of this article, proposition (**4.3**) can be used to improve results on the decomposition of de Bruijn digraphs into Hamilton circuits,

Proposition 4.4

- *If p is the greatest prime dividing d, then $\vec{\mathcal{B}}(d,2)$ contains $\frac{p-1}{p}d$ Hamilton circuits.*
- *$\vec{\mathcal{B}}(2^i q,2)$ contains $(2^i-1)q$ Hamilton circuits.*

Proof. The result holds for $p=1$. For $p>1$, by a result of D. Barth, J. Bond and A. Raspaud [6] we know that $\vec{\mathcal{B}}(p,2)$ contains $p-1$ arc-disjoint Hamilton circuits for p a prime, and has at least 4 vertices. Hence theorem (**4.3**) implies that, as $\vec{\mathcal{B}}(d,2)=\vec{\mathcal{B}}(pd_1,2)=\vec{\mathcal{B}}(d_1,2)\cdot\vec{\mathcal{B}}(p,2)$, $\vec{\mathcal{B}}(d,2)$ contains $(p-1)d_1$ arc-disjoint Hamilton circuits.

Similarly, the second result follows from a result of R. Rowley and B. Bose [14] stating that $\vec{\mathcal{B}}(2^i,2)$ contains 2^i-1 Hamilton circuits. □

4.3 Exhaustive Search for Hamilton decomposition of $\mathcal{WB}\mathcal{F}(p,2)$

As seen above the problem has been reduced to find a Hamilton decomposition of $\mathcal{WB}\mathcal{F}(p,2)=L(\vec{\mathcal{K}}_{p,p})$ for any prime $p\geq 5$. In order to provide ideas and to strengthen our conjecture we have performed some exhaustive searches. The complexity of an exhaustive search being exponential, we have restricted the set of solutions to the one such that *the i-th circuit H_i is obtained from H_0 by applying the automorphism ϕ_i of $\mathcal{WB}\mathcal{F}(p,2)$ which sends vertex (ab,l) to vertex $(a(b+i),l)$*. Furthermore we want solutions such that H_0 is Hamiltonian and the Hamilton circuits $H_i=\phi_i(H_0)$, $0\leq i\leq p-1$ are arc-disjoint. However the search space is still exponentional in p and a computer search (with normal computation resources) cannot be successful for p greater than 7. So we restricted again the search space to *"nearly linear"* solutions.

This restriction gave us solutions for small primes <29. For example for $p=5$ we found the cycle H_0 given by the following set of arcs:

$$\begin{array}{lcll}(ab,0) & \rightarrow & (a(2b),1) & \text{for } a\notin\{0,1\},\\ (0b,0) & \rightarrow & (0(2b+1),1),& \\ (1b,0) & \rightarrow & (1(2b+2),1),& \\ (ab,1) & \rightarrow & ((2a+b)b,0).&\end{array}$$

It induces the next cyclic permutation on level 0.

$$(00,11,14,20,40,30,10,42,24,23,01,33,21,12,31,32,04,44,13,03,22,34,43,41,02)$$

Finally we looked for very special Hamilton circuits H_0. That enabled us to find a solution for every prime p between 7 and 12000. More precisely, we searched for parameters α and β in $\mathbb{Z}_p$ such that H_0 is given by the following set of arcs:

$$\begin{array}{lcll}(ab,0) & \rightarrow & (a(\alpha b),1) & \text{for } a\neq 0,\\ (0b,0) & \rightarrow & (0(\alpha b+\beta),1),& \\ (ab,1) & \rightarrow & ((a+b+1)b,0).&\end{array}$$

One can easily check that if $\alpha \neq 1$ the H_i's are arc-disjoint. So we have only to find α and β such that H_0 is a Hamilton circuit. In particular we should have $\alpha \neq 0$ (condition to obtain a one difactor) and $\beta \neq 0$ (otherwise we obtain a circuit of length p starting at vertex $(0,0)$). We conjecture that:

Conjecture 7 *For any prime $p > 5$ there exist $\alpha \notin \{0,1\}$ and $\beta \neq 0$ such that the permutation π of $\mathbb{Z}_p^2$ defined by:*

$$\left.\begin{array}{rcll} \pi(ab) & = & (a+\alpha b+1)(\alpha b) & \text{if } a \neq 0, \\ \pi(0b) & = & (\alpha b+\beta+1)(\alpha b+\beta). & \end{array}\right\} \text{ is cyclic.}$$

The number of possible solutions is then only p^2. So we have been able to verify the conjecture, by a computer search for large values of p (≤ 12000). Below we give some solutions for p less than 100.

p	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
α	2	3	4	2	6	2	7	2	3	2	4	3	4	3	4	6	2	2	2	3	2	2
β	3	7	4	14	4	13	28	11	19	25	22	18	29	1	25	14	28	27	51	37	25	16

For example for $p = 7$, $\alpha = 2$, $\beta = 3$ we obtain the following cyclic permutation on level 0:

$$(00, 43, 46, 35, 03, 32, 14, 31, 62, 44, 61, 22, 04, 54, 01, 65, 33, 36, 25, 63, 66, 55, 23, 26, 15,$$
$$53, 56, 45, 13, 16, 05, 06, 21, 52, 34, 51, 12, 64, 11, 42, 24, 41, 02, 10, 20, 30, 40, 50, 60)$$

So using corollary (**4.3**) we have:

Theorem 4.5 *If d is divisible by any number q, $4 \leq q \leq 12000$ then $\mathcal{WB}\mathcal{F}(d,2)$ and consequently $\mathcal{WB}\mathcal{F}(d,n)$ has a Hamilton decomposition.*

This result can be strengthened in the case of $\mathcal{WB}\mathcal{F}(d,4)$. Indeed we know that $\mathcal{WB}\mathcal{F}(2,4)$ and $\mathcal{WB}\mathcal{F}(3,4)$ have a Hamilton decomposition and we have been able to generalize lemma (**4.2**) for $\vec{\mathcal{B}}(p,4) \cdot \vec{C}_n$ with p odd prime and $n \geq 5$.

Theorem 4.6 *If d is divisible by any number q, $2 \leq q \leq 12000$ then $\mathcal{WB}\mathcal{F}(d,4)$ and consequently $\mathcal{WB}\mathcal{F}(d,n)$ for $n \geq 4$ has a Hamilton decomposition.*

As a consequence the butterflies $\mathcal{WB}\mathcal{F}(2p,n)$ have an Hamilton decomposition for $n \geq 4$.

5 Conclusion

In this paper, we have shown that in a lot of cases Butterfly digraphs have a Hamilton decomposition and give strong evidence that the only exceptions should be $\mathcal{WB}\mathcal{F}(2,2)$, $\mathcal{WB}\mathcal{F}(2,3)$ and $\mathcal{WB}\mathcal{F}(3,2)$. We have furthermore reduced the problem to check if $L(\vec{\mathcal{K}}_{p,p})$ has a Hamilton decomposition for p prime (or equivalently that $\vec{\mathcal{K}}_{p,p}$ has an Eulerian compatible decomposition). We have also shown that such a decomposition will follow from the solution of a problem (conjecture (**7**)) in number theory. Our interest came from a conjecture of D. Barth and A. Raspaud [7] concerning the decomposition of

Butterfly networks into undirected Hamilton cycles. This conjecture is solved in [8] by generalizing the technics of section 3.2.

Finally we have seen in proposition (**4.4**) that the technics can be applied to obtain results on the Hamilton decomposition of de Bruijn digraphs. In the spirit it will be interesting to solve the following problem:

Problem: Determine the smallest integer $f_d(n)$ such that $\vec{\mathcal{B}}(d,n) \cdot \vec{C}_{f_d(n)}$ has a Hamilton decomposition.

A proof similar to that of lemma (**4.2**) should lead to $f_d(n) \leq n+1$. Conjecture (**6**) is, for a given d, equivalent to $f_d(n) \leq n$.

Acknowledgments

We thank very much J. Bond, R. Klasing, P. Paulraja, J.G. Peters and A. Raspaud for their remarks and comments which improve this paper.

References

[1] B. Alspach. Research problem 59. *Discrete Mathematics*, 50:115, 1984.

[2] B. Alspach, J-C. Bermond, and D. Sotteau. Decomposition into cycles I: Hamilton decompositions. In G. Hahn et al., editor, *Cycles and Rays, Proceeding Colloquium Montréal, 1987*, NATO ASI Ser. C, pages 9–18, Dordrecht, 1990. Kluwer Academic Publishers.

[3] J. Aubert and B. Schneider. Décomposition de la somme cartésienne d'un cycle et de l'union de deux cycles en cycles hamiltoniens. *Discrete Mathematics*, 38:7–16, 1982.

[4] R. Balakrishnan, J-C. Bermond, and P. Paulraja. On the decomposition of de bruijn graphs into hamiltonian cycles. Manuscript.

[5] D. Barth. *Réseaux d'interconnection: structures et communications*. PhD thesis, Université de Bordeaux I, 1994.

[6] D. Barth, J. Bond, and A. Raspaud. Compatible eulerian circuits in K_n^{**}. *Discrete Applied Mathematics*, 56:127–136, 1995.

[7] D. Barth and A. Raspaud. Two edge-disjoint hamiltonian cycles in the Butterfly graph. *Information Processing Letters*, 51:175–179, 1994.

[8] J-C. Bermond, E. Darrot, O. Delmas, and S. Perennes. Hamilton cycle decomposition of the Butterfly network. Technical Report RR-2920, Inria - Sophia Antipolis - Projet SLOOP (CNRS/INRIA/UNSA), June 1996. To appear in Parallel Processing Letters.

[9] J-C. Bermond, O. Favaron, and M. Maheo. Hamiltonian decomposition of Cayley graphs of degree 4. *Journal of Combinatorial Theory, Series B*, 46(2):142–153, 1989.

[10] J-C. Bermond and C. Peyrat. Broadcasting in de Bruijn networks. In Proceedings of the 19th S-E conference on Combinatorics, editor, *Congressus Numerantium 66*, pages 283–292. Graph theory, and Computing, Florida, 1988.

[11] S.J. Curran and J.A. Gallian. Hamilton cycles and paths in Cayley graphs and digraphs - a survey. To appear in Discrete Mathematics.

[12] H. Fleischner and B. Jackson. Compatible euler tours in eulerian digraphs. In G. Hahn et al., editor, *Cycles and Rays, Proceeding Colloquium Montréal, 1987*, pages 95–100. NATO ASI Ser. C, Kluwer Academic Publishers, Dordrecht, 1990.

[13] F. Thomson Leighton. *Introduction to Parallel Algorithms and Architectures: Arrays . Trees . Hypercubes*. Computer Science, Mathematics Electrical Engineering. Morgan Kaufmann Publishers, 1992.

[14] R. Rowley and B. Bose. On the number of arc-disjoint hamiltonian circuits in the de Bruijn graph. *Parallel Processing Letters*, 3(4):375–380, 1993.

[15] Jean de Rumeur. *Communication dans les réseaux de processeurs*. Collection Etudes et Recherches en Informatique. Masson, 1994. (English version to appear).

[16] M. Syska. *Communications dans les architectures à mémoire distribuée*. PhD thesis, Université de Nice Sophia Antipolis, 1992.

[17] T. Tillson. A Hamiltonian decomposition of K^*_{2m}, $2m \geq 8$. *Journal of Combinatorial Theory, Series B*, 29:68–74, 1980.

Contents

1 Introduction and notations

The construction of one, and if possible many edge-disjoint Hamilton cycles in a network can provide advantage for algorithms that make use of a ring structure. As example, the existence of many edge-disjoint Hamilton cycles allows the message traffic to be evenly distributed across the network. Furthermore, a partition of the edges into Hamilton cycles can be used in various distributed algorithms (termination, garbage collector, ...). So, many authors have considered the problem of finding how many edge-disjoint Hamilton cycles can be found in a given network. The most significant results have been obtained for the class of Cayley graphs on abelian groups, and for (underlying) line digraphs. Here we solve this problem for the *Butterfly networks*. These networks have been proposed as suitable topologies for parallel computers, due to their interesting structure (see [8, 9]) because they are, when properly defined, both Cayley digraphs (on a non-abelian group) and iterated line digraphs.

1.1 Definitions

First, we have to warn the reader that under the name *Butterfly* and with the same notation, different networks are described. Indeed, if some authors consider the *Butterfly network* as a multistage network used to route permutations, others consider it as a point-to-point network. In what follows, we will study the point-to-point version and use Leigthon's terminology [8], namely, *wrapped Butterfly*. Also, when we use the terms edge-disjoint or arc-disjoint, it obviously means *pairwise* edge-disjoint or arc-disjoint. In this article, we will use the next definitions and notations. For definitions not given here, see [9].

$\mathbb{Z}_q$ will denote the set of integers modulo q; addition of elements in $\mathbb{Z}_q$ will always occur in $\mathbb{Z}_q$.

Definition 1.1 *The* **wrapped Butterfly digraph** *of degree d and dimension n, denoted $W\vec{\mathcal{B}}\mathcal{F}(d,n)$, has as vertices the couples (x,l) where x is an element of $\mathbb{Z}_d^n$, that is, a word $x_{n-1}x_{n-2}\cdots x_1x_0$ where the letters belong to $\mathbb{Z}_d$, and $l \in \mathbb{Z}_n$ (l is called the level). For any l, a vertex labelled $(x_{n-1}x_{n-2}\cdots x_l\cdots x_1x_0, l)$ is joined by an arc to d vertices labelled $(x_{n-1}\cdots x_{l+1}, x_l+\alpha, x_{l-1}\cdots x_0, l+1)$ where α is any element of $\mathbb{Z}_d$. Each one of these arcs is said to have the* **slope** *α.*

$W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is a d-regular digraph with nd^n vertices; its diameter is $2n-1$. This network is sometimes considered as undirected, but its structure being indeed directed, we will always consider the digraph.

For convenience, we repeat the level 0 when drawing the wrapped Butterfly digraph. Hence, the reader has to remember that the two occurrences of level 0 have to be identified. Figure (**1**) displays $W\vec{\mathcal{B}}\mathcal{F}(3,2)$ with the arcs directed from left to right. Note that $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is often represented (for example in [8, 9]) in an opposite way to our drawing as the authors denote the nodes $(x_0x_1\cdots x_{n-1}, l)$.

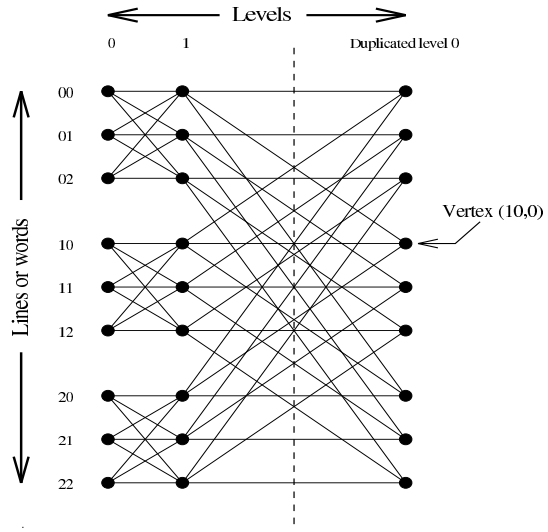

Figure 1: *The digraph $\vec{\mathcal{WBF}}(3,2)$, the arcs beings directed from left to right.*

Now, we give two digraph definitions we use in the following.

- $\mathcal{K}_d^+$ will denote the complete symmetric digraph with a loop on each vertex,
- $\vec{\mathcal{K}}_{d,d}$ will denote the complete bipartite digraph where each set of the bipartition has size d and with all the arcs directed from the left part to the right part.

Note that $\vec{\mathcal{WBF}}(d,1)$ is nothing else than $\mathcal{K}_d^+$.

In digraphs, the concept of dipaths and circuits (directed cycles) is well-known. Here, we need to use more general concepts valid for digraphs of paths and cycles (which are also called oriented elementary paths and oriented elementary cycles).

Definition 1.2 *A* **path of a digraph** *is a sequence $\mu = (v_0, e_0, v_1, e_1, \cdots, v_k, e_k, v_{k+1})$ where the v_i's are vertices and the e_i's are arcs such that the end vertices of e_i are v_i and v_{i+1} and where the sequence μ does not meet twice the same vertex except maybe v_0 and v_{k+1}.*

Definition 1.3 *A path such that $v_{k+1} = v_0$ in the sequence μ is called a* **cycle**.

Note that the arc e_i can be either directed from v_i to v_{i+1} or from v_{i+1} to v_i. If all the arcs of the path (*resp. cycle*) are directed from v_i to v_{i+1} we have a dipath (*resp. circuit also called dicycle*).

Definition 1.4 *A vertex v_i of a cycle is said to be* **of type +** *(*resp. **of type −***) for the cycle, if v_i is the terminal vertex of e_{i-1} (*resp. e_i*) and the initial vertex of e_i (*resp. e_{i-1}*).*

Note that in a circuit, all vertices are of type +, but the type is not necessarily defined for all the vertices of a cycle.

Definition 1.5 *A vertex v is said* **to be crossed by a cycle**, *or* **a cycle crosses the vertex** *v, if v is of type + or of type − for the cycle. When a vertex v is crossed by a cycle, we will define its* **sign function** *ϵ by $\epsilon(v) = +1$ (*resp. *$\epsilon(v) = -1$) if v is of type +* (resp. of type *−*).

Remark 1 We can also define the predecessor $p(v)$ and the successor $s(v)$ of the vertex v in the order induced by the cycle. Then, the vertex v is of type + (or has sign $\epsilon(v) = +1$) if $(p(v), v)$ and $(v, s(v))$ are both arcs of the digraph, and is of type − (or has sign $\epsilon(v) = -1$) if both $(s(v), v)$ and $(v, p(v))$ are arcs of the digraph.

Definition 1.6 *A* **Hamilton cycle** *(*resp. **circuit**) of a digraph is a cycle (*resp. circuit*) which contains every vertex exactly once.*

Definition 1.7 *We will say that a digraph is* **decomposable into Hamilton cycles** *(*resp. **circuits**) if its arcs can be partitioned into Hamilton cycles (*resp. circuits*).*

Definition 1.8 *A Hamilton cycle of $W\vec{B}F(d, n)$ will be said to be* **l-crossing** *if the cycle crosses all the vertices of level l and furthermore $\sum_{v=(x,l),\, x\in\mathbb{Z}_d^n} \epsilon(v) \equiv 0 \pmod{d}$.*

Figure (**3**) shows examples of 1-crossing Hamilton cycles in $W\vec{B}F(3,2)$ and $W\vec{B}F(3,3)$.

1.2 Results

Various results have been obtained on the existence of Hamilton cycles in classical networks (see for example the surveys [2, 7]). For example, it is well-known that any Cayley graph on an abelian group is hamiltonian. Furthermore, it has been conjectured by Alspach [1] that:

Conjecture 1 (Alspach) *Every connected Cayley graph on an abelian group has a Hamilton decomposition.*

This conjecture has been verified for all connected 4-regular graphs on abelian groups in [6]. It includes in particular the toroidal meshes (grids). For the hypercube, it is also known that $\mathcal{H}(2d)$ is decomposable into d Hamilton cycles (see [2, 3]).

The wrapped Butterfly digraph is actually a Cayley graph (on a non-abelian group) and a line digraph. So, the decomposition into Hamilton cycles (*resp. circuits*) of this digraph has received some attention. It is well-known that $W\vec{B}F(d, n)$ has one Hamilton circuit (see [8, page 465] for a proof in the case $d = 2$ or [12]). In [4], Barth and Raspaud proved that the

underlying multigraph associated to $W\vec{\mathcal{B}}\mathcal{F}(2,n)$ contains two arc-disjoint Hamilton cycles answering a conjecture of J. Rowley and D. Sotteau [10]. In our terminology, their result can be stated as:

Theorem 1.1 (Barth, Raspaud) *$W\vec{\mathcal{B}}\mathcal{F}(2,n)$ is decomposable into Hamilton cycles.*

They conjectured that this result can be generalized for any degree:

Conjecture 2 (Barth, Raspaud) *For $n \geq 2$, $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is decomposable into Hamilton cycles.*

In this paper, we prove the conjecture (**2**). To do so, we use some techniques introduced in [5] where we studied the decomposition of $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ into Hamilton circuits. In fact, we prove that $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is decomposable into d l-crossing Hamilton cycles. Indeed, the l-crossing property, combined with the recursive structure of $W\vec{\mathcal{B}}\mathcal{F}(d,n)$, enables us to prove that the number of l-crossing arc-disjoint Hamilton cycles that $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ contains can only increase when n increases. Then, we prove mainly that $W\vec{\mathcal{B}}\mathcal{F}(d,2)$ contains d arc-disjoint l-crossing Hamilton cycles, by constructing two arc-disjoint l-crossing Hamilton cycles using only arcs of slopes 0 and 1 and $d-2$ arc-disjoint Hamilton circuits using arcs of other slopes. These results are summarized in the following theorem:

Theorem 1.2 *For $n \geq 2$,*

- *for $d \notin \{3,4,6\}$, $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is decomposable into $d-2$ Hamilton circuits and 2 Hamilton cycles,*
- *for $d \in \{4,6\}$, $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is decomposable into Hamilton circuits,*
- *$W\vec{\mathcal{B}}\mathcal{F}(3,n)$ is decomposable into 1 Hamilton circuit and 2 Hamilton cycles.*

2 The general construction

We give below some additional definitions and properties enabling us to establish the lemma (**2.2**) which is indeed a strengthened version of the inductive lemma of [5]. This lemma is then applied in section (**3**) to construct inductively the decomposition.

2.1 Families of perfect matchings

We will denote by M a permutation of $\mathbb{Z}_d$ mapping a to $M(a)$ or equivalently the associated perfect matching of $\vec{\mathcal{K}}_{d,d}$ which contains all the arcs $(a, M(a))$.

Definition 2.1 *Let S be a set of slopes (that is a subset of $\mathbb{Z}_d$). Then, a* **perfect matching** *M of $\vec{\mathcal{K}}_{d,d}$* **uses the slopes in S** *if, for any $a \in \mathbb{Z}_d$ $M(a) \in \{a+s,\ s \in S\}$. A* **family of perfect matchings** *$\mathcal{M} = \{M_x,\ x \in \mathbb{Z}_d^n\}$ of $\vec{\mathcal{K}}_{d,d}$* **uses the slopes in S** *if, for any perfect matching M_x of the family, M_x uses the slopes in S.*

Definition 2.2 *For $1 \leq j \leq p$, let $\mathcal{M}_j = \{M_{x,j} \,|\, x \in \mathbb{Z}_d^n\}$ be p families of perfect matchings. The* **families** *$\mathcal{M}_j$ are said to be* **compatible** *if, for each x in $\mathbb{Z}_d^n$, the perfect matchings $M_{x,j}$ are arc-disjoint (i.e. $\forall a \;\; M_{x,j}(a) \neq M_{x,j'}(a)$, for $j \neq j'$).*

Definition 2.3 *A family $\mathcal{M} = \{M_x,\ x \in \mathbb{Z}_d^n\}$ of $\vec{\mathcal{K}}_{d,d}$ perfect matchings satisfies the* **cyclic-potent property** *if, for any order of composition of the M_x and any set of sign $\{\epsilon_x \mid x \in \mathbb{Z}_d^n,\ \epsilon_x \in \{-1, 1\}\}$ such that $\sum_x \epsilon_x \equiv 0$ mod d, the permutation $\Pi_x M_x^{\epsilon_x}$ is cyclic.*

Definition 2.4 *A* **family of perfect matchings** *$\mathcal{M} = \{M_x,\ x \in \mathbb{Z}_d^n\}$ is* **of type** *(i, j) if:*

- *for $x \neq 0$, $M_x(a) = a + i$;*
- *for $x = 0$, $M_0(a) = a + j$.*

Lemma 2.1 *A family of perfect matchings of type (i, j) $\mathcal{M} = \{M_x, x \in \mathbb{Z}_d^n\}$ is cyclic-potent if and only if $j - i$ is prime with d.*

Proof. As the permutations of the family commute, the permutation $\Pi_x M_x^{\epsilon_x}$ of definition (**2.3**) can be simply expressed as $x \to x + \delta$. So, this permutation will be cyclic if and only if δ is prime with d. Here $\delta = (\sum_{x \neq 0} \epsilon_x)i + \epsilon_0 j$. As $\sum_x \epsilon_x = 0$, we have $\delta = (\sum_x \epsilon_x)i + \epsilon_0(j - i) = \epsilon_0(j - i)$. So, δ is clearly prime with d if and only if $j - i$ is prime with d. □

In section (**3**), we will need some very simple cyclic-potent families of perfect matchings that we give as examples. We will represent a set of p families of perfect matchings of type (i, j):

$$\{(i_0, j_0), (i_1, j_1), \ldots, (i_{p-1}, j_{p-1})\}$$

by the array:

$$\begin{array}{cccccccc} i_0 & i_1 & i_2 & i_3 & \ldots & i_{p-2} & i_{p-1} \\ j_0 & j_1 & j_2 & j_3 & \ldots & j_{p-2} & j_{p-1} \end{array}$$

Families 1 There exist d compatible cyclic-potent families of perfect matchings:

$$\begin{array}{cccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & \ldots & d-2 & d-1 \\ 1 & 2 & 3 & 4 & 5 & 6 & \ldots & d-1 & 0 \end{array}$$

These families are cyclic-potent as, applying lemma (**2.1**), we obtain:

$$1 - 0 = 2 - 1 = \cdots = d - 1 - (d - 2) = 0 - (d - 1) = 1$$

which is prime with d. These families use all the slopes.

Families 2 There exist 2 compatible families which use the slopes $\{0,1\}$:

$$\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}$$

According to lemma (**2.1**), they are two compatible cyclic-potent families and they use the slopes $\{0,1\}$.

Families 3 When $d \neq 3$, there exist $d-2$ compatible cyclic-potent families of perfect matchings using the slopes $\{2,\ldots,d-1\}$. One possible solution is given below:

- When d is odd and $d \neq 3$, the following families can be used:

$$\begin{array}{ccccccccc} 2 & 3 & 4 & 5 & \ldots & d-3 & d-2 & d-1 \\ 4 & 5 & 6 & 7 & \ldots & d-1 & 2 & 3 \end{array}$$

- When d is even, we use the following families:

$$\begin{array}{cccccccc} 2 & 3 & 4 & 5 & \ldots & d-2 & d-1 \\ 3 & 2 & 5 & 4 & \ldots & d-1 & d-2 \end{array}$$

These families are cyclic-potent as, applying lemma (**2.1**), we get:

- for d odd:

$$\begin{array}{ccccccccccc} 4-2 & = & 5-3 & = & \cdots & = & d-1-(d-3) & = & 2 \\ & & \text{and} & & 2-(d-2) & = & 3-(d-1) & = & 4 \end{array}$$

  as 2 and 4 are prime with d;

- for d even:

$$\begin{array}{ccccccccccc} & 3-2 & = & 5-4 & = & \cdots & = & (d-1)-(d-2) & = & 1 \\ \text{and} & 2-3 & = & 4-5 & = & \cdots & = & (d-2)-(d-1) & = & -1 \end{array}$$

  which are prime with d.

In both cases, the slopes used are in $\{2,\ldots,d-1\}$.

2.2 Inductive construction

Lemma 2.2 *If $\mathcal{WBF}(d,n)$ admits p arc-disjoint l-crossing Hamilton cycles and if there exist p cyclic-potent families of perfect matchings in $\vec{\mathcal{K}}_{d,d}$, then $\mathcal{WBF}(d,n+1)$ admits p arc-disjoint l-crossing Hamilton cycles.*

Proof. Let H be an l-crossing Hamilton cycle of $\mathcal{WB}\mathcal{F}(d,n)$. As all the levels are equivalent, we can suppose without loss of generality and for simplicity in the notations that $l=0$. Let $\mathcal{M}=\{M_x,\ x\in\mathbb{Z}_d^n\}$ be a cyclic-potent family of perfect matchings of $\vec{\mathcal{K}}_{d,d}$. The vertices of $\mathcal{WB}\mathcal{F}(d,n+1)$ can be labeled (ax,l) with $a\in\mathbb{Z}_d, x\in\mathbb{Z}_d^n$ and $l\in\mathbb{Z}_{n+1}$. Now, we associate to H and $\mathcal{M}$ a partial digraph H' in $\mathcal{WB}\mathcal{F}(d,n+1)$ as follows (for an example of such a construction see figure (**3**)):

- for $0\leq l\leq n-1$ and for each a, if the arc $(x,l)(x',l+1)$ belongs to H, we put in H' the arc $(ax,l)(ax',l+1)$ where the indices are taken modulo $n+1$, which means that to the arc $(x,n-1)(x',0)$ of H is associated the arc $(ax,n-1)(ax',n)$ in H';
- between levels n and 0 of $\mathcal{WB}\mathcal{F}(d,n+1)$ we put the arcs joining (ax,n) to $(M_x(a)x,0)$.

With such a definition, each vertex of $\mathcal{WB}\mathcal{F}(d,n+1)$ is incident to two arcs of H'. Hence, we can define for each vertex a predecessor and a successor on H' that enables us to prove that we can order H' in a cycle.

For $1\leq l\leq n-1$, let (x',l') (*resp.* (x'',l'')) be the predecessor (*resp. successor*) of (x,l) in H; then, the predecessor (*resp. successor*) of (ax,l) in H' will be (ax',l') (*resp.* (ax'',l'')).

For $l=0$ and n, as H is a 0-crossing Hamilton cycle, vertices $(x,0)$ are either of type $+$ or $-$ on H.

When $(x,0)$ is of type $+$, its predecessor (*resp. successor*) in the cycle H is $(x',n-1)$ (*resp.* $(x'',1)$). Then, in H' the predecessor (*resp. successor*) of (ax,n) will be $(ax',n-1)$ (*resp.* $(M_x(a)x,0)$); the predecessor (*resp. successor*) of $(ax,0)$ will be $(M_x^{-1}(a)x,n)$ (*resp.* $(ax'',1)$).

When $(x,0)$ is of type $-$, its predecessor (*resp. successor*) in H is $(x',1)$ (*resp.* $(x'',n-1)$). Then, in H' the predecessor (*resp. successor*) of $(ax,0)$ will be $(ax',1)$ (*resp.* $(M_x^{-1}(a)x,n)$); the predecessor (*resp. successor*) of (ax,n) will be $(M_x(a)x,0)$ (*resp.* $(ax'',n-1)$) in H'.

Therefore, when $(x,0)$ is of type $+$ (*resp.* $-$), (ax,n) and $(ax,0)$ are vertices of type $+$ (*resp.* $-$) in H'. Hence, all the vertices of levels 0 and n are crossed by H'; furthermore, the sum of the signs of the vertices of H' of levels 0 or n will be d times the sum of the signs of the vertices of H of level 0, that is, by hypothesis, 0. Hence, H' is 0-crossing (and also n-crossing).

Now, we have to prove that H' is effectively a Hamiltoncycle. For this, it suffices to prove that if we start at some vertex $(ax,0)$ and follow H', we meet successively all the vertices of level 0 and n before coming back to $(ax,0)$. Indeed, suppose that (y,l) was on the portion of cycle H between $(x_1,0)$ and $(x_2,0)$. Then, (ay,l) will be on the portion of H' between (ax_1,α) and (ax_2,β), where $\alpha=0$ (*resp.* $\alpha=n$) if $(x_1,0)$ is of type $+$ (*resp.* $-$), and $\beta=0$ (*resp.* $\beta=n$) if $(x_2,0)$ is of type $-$ (*resp.* $+$). These cases are described on figure (**2**).

Now, let $(x_0,0),(x_1,0),\ldots,(x_{d^n}=x_0,0)$ be the sequence of vertices of H at level 0 in the order we meet them on H. Starting from $(a_0x_0,0)$, we will meet successively $(a_1x_1,0)$, $(a_2x_2,0)$, ... and $(a_{d^n}x_{d^n}=a_{d^n}x_0,0)$ on H'. Following such a path, we can meet either x_i of type $+$ by going from level n to level 0, in which case we will apply the perfect matching M_{x_i} to some a, or x_i of type $-$ by going from level 0 to n, in which case we will apply $M_{x_i}^{-1}$ to a. So, $a_{d^n}=\Pi M_{x_i}^{\epsilon_{x_i}}(a)$ where the product is taken in an order depending on x_0. As all the x_i differ, we can meet again $(a_0x_0,0)$ only at some $a_{qd^n}x_0$, but M being cyclic-potent, the values $a_{d^n},a_{2d^n},\ldots,a_{qd^n},\ldots,a_{(d)d^n}$ are all distinct. So, we meet again $(a_0x_0,0)$ only after having encountered the d^{n+1} vertices of level 0.

Now, note that we can perform this construction with p arc-disjoint 0-crossing cycles and p compatible cyclic-potent families. From construction, the p 0-crossing cycles that we will obtain will be arc-disjoint. □

Remark 2 When the 0-crossing Hamilton cycles used in the lemma above are circuits of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$, all the vertices are of type $+$, and the construction leads to circuits of $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n+1)$, giving another proof of the inductive lemma of [5].

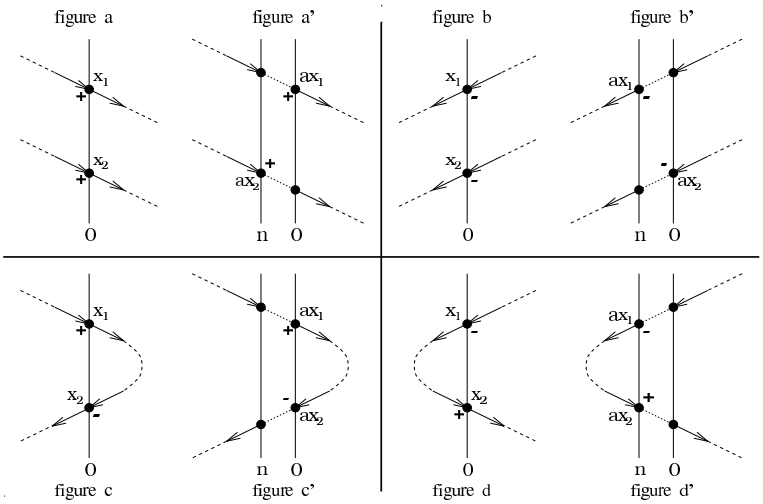

Figure 2: *This figure shows the four possible cases when we perform the inductive construction of* $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n+1)$ *from* $\mathcal{W}\vec{\mathcal{B}}\mathcal{F}(d,n)$. *In figure a and a'* (resp. *b* and *b'*) *the vertices* x_1 *and* x_2 *are of type* $+$ (resp. $-$). *Figure c and c'* (resp. *d* and *d'*) *displays the case where the vertex* x_1 *is of type* $+$ (resp. $-$) *and the vertex* x_2 *is of type* $-$ (resp. $+$).

3 Decomposition of $\vec{\mathcal{WBF}}(d,n)$

We will use a decomposition of $\vec{\mathcal{WBF}}(d,n)$ into two partial digraphs.

Definition 3.1 *The Butterfly digraph $\vec{\mathcal{WBF}}(d,n)$ is the sum of* **two partial digraphs** *$\vec{\mathcal{WBF}}_{0,1}(d,n)$ and $\vec{\mathcal{WBF}}_{2,\ldots,d-1}(d,n)$ defined as follows:*

- *$\vec{\mathcal{WBF}}_{0,1}(d,n)$ contains the arcs which slopes belong to $\{0,1\}$,*
- *$\vec{\mathcal{WBF}}_{2,\ldots,d-1}(d,n)$ contains the arcs which slopes belong to $\{2,\ldots,d-1\}$.*

3.1 Decomposition of $\vec{\mathcal{WBF}}_{2,\ldots,d-1}(d,n)$

The proof is inductive on n. We start the induction for $n=1$.

Lemma 3.1 *When $d \notin \{4,6\}$, $\vec{\mathcal{WBF}}_{2,\ldots,d-1}(d,1)$ is decomposable into Hamilton circuits.*

Proof. As $\vec{\mathcal{WBF}}(d,1) = K_d^+$, $\vec{\mathcal{WBF}}_{2,\ldots,d-1}(d,1)$ is obtained from K_d^+ by removing the loops and the arcs of slope 1. Following Tillson [11], we know that K_d^+ without the loops contains $d-1$ arc-disjoint Hamilton circuits when $d \neq 4,6$. So, using Tillson decomposition, we can label the vertices of K_d^+ such that one of the circuits uses all the arcs of slope 1. By removing it we get $d-2$ arc-disjoint Hamilton circuits in $\vec{\mathcal{WBF}}_{2,\ldots,d-1}(d,1)$. □

Proposition 3.1 *For $d \notin \{3,4,6\}$, $\vec{\mathcal{WBF}}_{2,\ldots,d-1}(d,n)$ is decomposable into Hamilton circuits.*

Proof. As $d \notin \{4,6\}$, the proposition is proved for $n=1$ by lemma (**3.1**). Then, as $d \neq 3$, the $d-2$ compatible cyclic-potent families (**3**) in section (**2.1**) use the slopes $\{2,\ldots,d-1\}$ and satisfy the hypothesis of lemma (**2.2**). Hence, we can apply that lemma inductively, in order to construct $d-2$ arc-disjoint Hamilton circuits (see remark (**2**)) in $\vec{\mathcal{WBF}}_{2,\ldots,d-1}(d,n)$. □

3.2 Decomposition of $\vec{\mathcal{WBF}}_{0,1}(d,n)$

Lemma 3.2 *$\vec{\mathcal{WBF}}_{0,1}(d,2)$ is decomposable into l-crossing Hamilton cycles.*

Proof. For this proof, the vertices of $\vec{\mathcal{WBF}}_{0,1}(d,2)$ will be denoted by the couples (xy,l) with $x \in \mathbb{Z}_d$, $y \in \mathbb{Z}_d$ and $l \in \mathbb{Z}_2$. We will show that we can build two arc-disjoint 1-crossing Hamilton cycles in $\vec{\mathcal{WBF}}_{0,1}(d,2)$ by using two sets of arcs of $\vec{\mathcal{WBF}}_{0,1}(d,2)$ defined by the next two rules:

1. *Arcs of H_0:*

$$\begin{cases} \text{if } x \neq y, & (x(y-1),0) \overset{+1}{\rightarrow} (xy,1) \overset{+0}{\rightarrow} (xy,0), & (1) \\ \text{if } x = y, & (xx,0) \overset{+0}{\rightarrow} (xx,1) \overset{+1}{\rightarrow} ((x+1)x,0). & (2) \end{cases}$$

2. *Arcs of H_1:*

$$\begin{cases} \text{if } x \neq y, & (xy,0) \overset{+0}{\rightarrow} (xy,1) \overset{+1}{\rightarrow} ((x+1)y,0), & (1) \\ \text{if } x = y, & (x(x-1),0) \overset{+1}{\rightarrow} (xx,1) \overset{+0}{\rightarrow} (xx,0). & (2) \end{cases}$$

It is easy to verify that H_0 and H_1 are arc-disjoint. With the arcs (1) of H_0, we can define for each $x \in \mathbb{Z}_d$ a dipath P_x as follows:

$$P_x \begin{cases} & (xx,0) & \rightarrow & (x(x+1),1) & \rightarrow & (x(x+1),0) & \rightarrow \\ \rightarrow & (x(x+2),1) & \rightarrow & \cdots & \rightarrow & (x(x+d-2),1) & \rightarrow \\ \rightarrow & (x(x+d-2),0) & \rightarrow & (x(x+d-1),1) & \rightarrow & (x(x+d-1),0) & \end{cases}$$

The d dipaths P_x, $x \in \mathbb{Z}_d$, are clearly vertex-disjoint. Only the vertices noted $(xx,1)$ are not in these d dipaths. The arcs (2) of H_0 allows us to join the end vertices of the d dipaths through the missing vertices $(xx,1)$ as follows:

$$\begin{array}{lllll} P_x & \leftarrow & ((x+d-1)(x+d-1),1) & \leftarrow & P_{x+d-1} \leftarrow \\ & \leftarrow & ((x+d-2)(x+d-2),1) & \leftarrow & \cdots \leftarrow \\ & \leftarrow & ((x+1)(x+1),1) & \leftarrow & P_{x+1} \leftarrow \\ & \leftarrow & (xx,1) & \leftarrow & P_x \end{array}$$

One can easily check that we have defined a Hamilton cycle. The d dipaths are joined through their extremal vertices in a cyclic way, using only arcs (2) of H_0.

By construction, all the vertices at level 1 are crossed. In order to compute the sign of the vertices at level 1, we can choose to walk along the cycle in the direction $(xx,0) \rightarrow (x(x+1),1)$. Therefore, all the vertices $(xy,1)$ with $x \neq y$ are of type $+$ and have $+1$ as sign, while the vertices $(xx,1)$ are of type $-$ and have -1 as sign. So, the sum of the signs is $(d^2-d)-(d) \equiv 0 \pmod{d}$.

To prove that the second set of rules builds a second 1-crossing Hamilton cycle, it suffices to notice that we can rewrite this rule up to a permutation of the letters x and y as being:

- *Arcs of H_1 (with permutation of x and y):*

$$\begin{cases} \text{if } y \neq x, & (y(x+1),0) \overset{+1}{\leftarrow} (yx,1) \overset{+0}{\leftarrow} (yx,0), \\ \text{if } y = x, & (yy,0) \overset{+0}{\leftarrow} (yy,1) \overset{+1}{\leftarrow} ((y-1)y,0). \end{cases}$$

Construction (2) is then clearly similar to construction (1); to be convinced, just exchange x and y, and replace 1 by -1 in the proof for construction (1).

Hence, H_0 and H_1 are two arc-disjoint 1-crossing Hamilton cycles. As the levels are equivalent, the result holds also for level 0. □

Figure (**3**) gives a decomposition of $\mathcal{WB}\vec{\mathcal{F}}_{0,1}(3,2)$ into two 1-crossing Hamilton cycles.

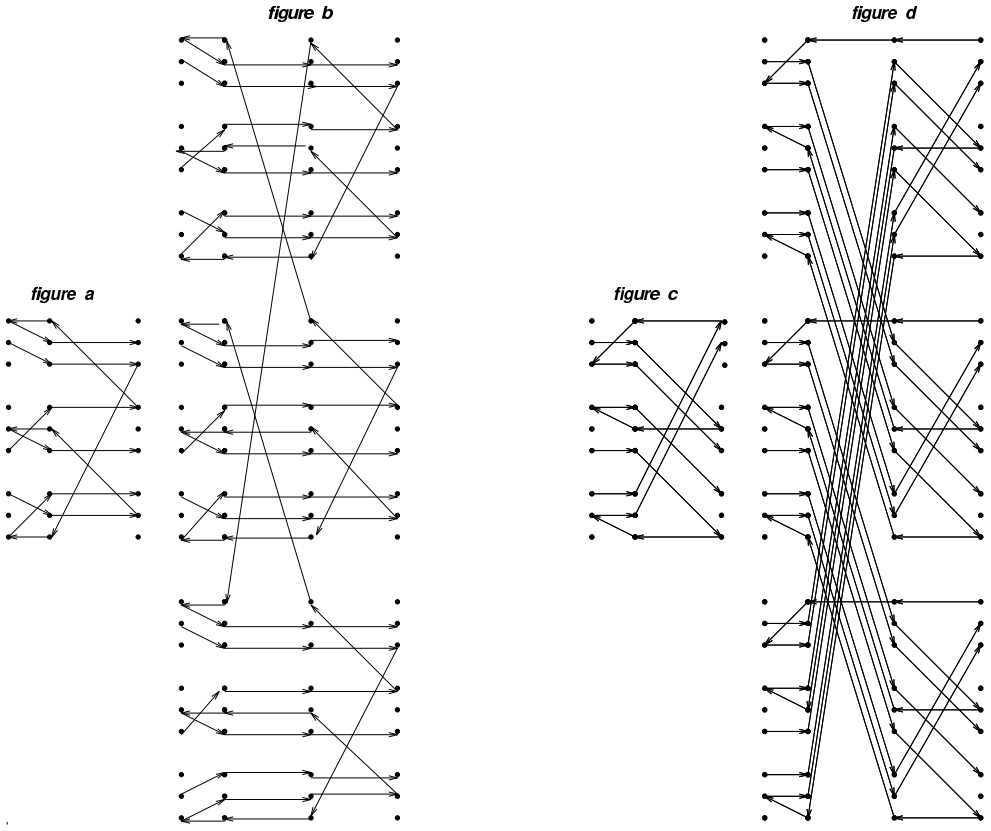

Figure 3: *Figures a and c show the two* 1*-crossing arc-disjoint Hamilton cycles of* $\mathcal{WB}\vec{\mathcal{F}}_{0,1}(3,2)$*. We display on figures b and d, two* 1*-crossing arc-disjoint Hamilton cycles in* $\mathcal{WB}\vec{\mathcal{F}}_{0,1}(3,3)$ *obtained by applying lemma (***2.2***) with the families (***2***).*

Proposition 3.2 *For* $n \geq 2$, $\mathcal{WB}\vec{\mathcal{F}}_{0,1}(d,n)$ *is decomposable into* l*-crossing Hamilton cycles.*

Proof. The proposition is proved for $n = 2$ by the lemma (**3.2**). Then, we use lemma (**2.2**) with the two compatible cyclic-potent families (**2**) in section (**2.1**) which use

the slopes $\{0,1\}$ to construct inductively two arcs-disjoint l-crossing Hamilton cycles in $W\vec{\mathcal{B}}\mathcal{F}_{0,1}(d,n)$. □

Figure (**3**) gives the recursive construction of two 1-crossing arc-disjoint Hamilton cycles in $W\vec{\mathcal{B}}\mathcal{F}_{0,1}(3,3)$ from two 1-crossing arc-disjoint cycles in $W\vec{\mathcal{B}}\mathcal{F}(3,2)$.

3.3 Global Decomposition

We are now ready to prove the main result:

Theorem 3.3 *For $n \geq 2$,*

- *for $d \notin \{3,4,6\}$, $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is decomposable into $d-2$ Hamilton circuits and 2 Hamilton cycles,*
- *for $d \in \{4,6\}$, $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is decomposable into Hamilton circuits,*
- *$W\vec{\mathcal{B}}\mathcal{F}(3,n)$ is decomposable into 1 Hamilton circuit and 2 Hamilton cycles.*

Proof. According to propositions (**3.1**) and (**3.2**) we have, when $d \notin \{3,4,6\}$, $d-2$ arc-disjoint circuits in $W\vec{\mathcal{B}}\mathcal{F}_{2,\ldots,d-1}(d,n)$ and 2 arc-disjoint cycles in $W\vec{\mathcal{B}}\mathcal{F}_{0,1}(d,n)$. So, the result holds in these cases. For $d \in \{4,6\}$ and $n=2$, an exhaustive computer search shows that $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is decomposable into Hamilton circuits, and so, for $n \geq 2$, $W\vec{\mathcal{B}}\mathcal{F}(4,n)$ and $W\vec{\mathcal{B}}\mathcal{F}(6,n)$ are decomposable into Hamilton circuits. For $d=3$, we can construct two 1-crossing arc-disjoint Hamilton cycles and one arc-disjoint Hamilton circuit in $W\vec{\mathcal{B}}\mathcal{F}(3,2)$ (see figure (**4**)). Then, we can apply lemma (**2.2**) with families (**1**) and the result holds for $W\vec{\mathcal{B}}\mathcal{F}(3,n)$ with $n \geq 2$. □

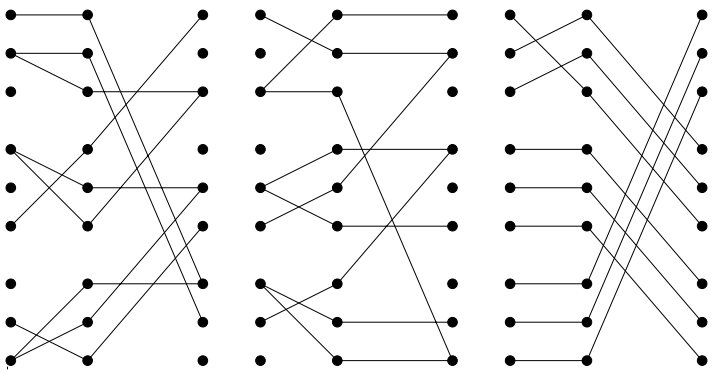

Figure 4: *The decomposition of $W\vec{\mathcal{B}}\mathcal{F}(3,2)$ into two 1-crossing arc-disjoint Hamilton cycles and one arc-disjoint Hamilton circuit.*

The preceding result implies the conjecture of Barth and Raspaud:

Theorem 3.4 *For any d and $n \geq 2$, $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is decomposable into Hamilton cycles.*

Remark 3 We could also have derived theorem (**3.4**) by proving that, if $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is decomposable into l-crossing Hamilton cycles, then $W\vec{\mathcal{B}}\mathcal{F}(d,n+1)$ is also decomposable into l-crossing Hamilton cycles. This can be done by applying lemma (**2.2**) with the families (**1**) in section (**2.1**). But to start the induction we needed to split the Butterfly digraph into two partial digraphs in order to prove that $W\vec{\mathcal{B}}\mathcal{F}(d,2)$ is decomposable into l-crossing Hamilton cycles for $n = 2$ and $d \neq 3$.

4 Conclusion

In this paper we have proved that $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ is always decomposable into Hamilton cycles. However, the problem of decomposing $W\vec{\mathcal{B}}\mathcal{F}(d,n)$ into Hamilton circuits remains open and is considered in [5]. The difficulty in that case is to start the induction. In fact, we conjecture that $W\vec{\mathcal{B}}\mathcal{F}(d,2)$ is decomposable into Hamilton circuits for $d > 3$. Unfortunately such a decomposition is not yet known, even if in [5] we were able to reduce the problem to the case d prime and to solve it in many cases. Consequently, we propose as open problem the following conjecture:

Conjecture 3 ([5]) *For any prime number $p > 3$, $W\vec{\mathcal{B}}\mathcal{F}(p,2)$ is decomposable into Hamilton circuits.*

Proving this conjecture would completely close the problem of the Hamilton decomposition of the Butterfly network.

References

[1] B. Alspach. Research problem 59. *Discrete Mathematics*, 50:115, 1984.

[2] B. Alspach, J-C. Bermond and D. Sotteau. Decomposition into cycles I: Hamilton decompositions. In G. Hahn et al., editors, *Cycles and Rays*, vol. 301 of *NATO ASI Series C: Mathematical and Physical Sciences*, pp. 9–18. Kluwer Academic Publishers, Dordrecht, 1990. Proceedings of the NATO Advance Research Workshop on Cycles and Rays: Basic Structures in Finite and Infinite Graphs, Montréal, May 3-9, 1987.

[3] J. Aubert and B. Schneider. Décomposition de la somme cartésienne d'un cycle et de l'union de deux cycles en cycles hamiltoniens. *Discrete Mathematics*, 38:7–16, 1982.

[4] D. Barth and A. Raspaud. Two edge-disjoint hamiltonian cycles in the Butterfly graph. *Information Processing Letters*, 51:175–179, 1994.

[5] J-C. Bermond, E. Darrot, O. Delmas and S. Perennes. Hamilton circuits in the directed Butterfly network. Research Report #2925 — Theme 1, INRIA Sophia Antipolis, July 1996. Submitted to *Discrete Applied Mathematics.*

[6] J-C. Bermond, O. Favaron and M. Maheo. Hamiltonian decomposition of Cayley graphs of degree 4. *Journal of Combinatorial Theory*, series B, 46(2):142–153, 1989.

[7] S. J. Curran and J. A. Gallian. Hamilton cycles and paths in Cayley graphs and digraphs - a survey. To appear in *Discrete Mathematics.*

[8] F. Thomson Leighton. *Introduction to Parallel Algorithms and Architectures: Arrays . Trees . Hypercubes.* Computer Science, Mathematics, Electrical Engineering. Morgan Kaufmann Publishers, 1992.

[9] Jean de Rumeur. *Communications dans les réseaux de processeurs.* Collection études et recherches en informatique. Masson, Paris, 1994. English version to appear.

[10] D. Sotteau and J. Rowley. Private communication.

[11] T. Tillson. A Hamiltonian decomposition of K^*_{2m}, $2m \geq 8$. *Journal of Combinatorial Theory*, series B, 29:68–74, 1980.

[12] S. A. Wong. Hamilton Cycles and Paths in Butterfly Graphs. *Networks*, 26(3):145–150, October 1995.